Edge-corE®

ECS4310-26T
26-Port
Gigabit Smart Switch

Management Guide

www.edge-core.com

MANAGEMENT GUIDE

ECS4310-26T GIGABIT SMART SWITCH

with 24 10/100/1000BASE-T (RJ-45) Ports,
and 2 Gigabit SFP Slots

ECS4310-26T
E072010-CS-R01
149100000083A

About This Guide

Purpose This guide gives specific information on how to operate and use the management functions of the switch.

Audience The guide is intended for use by network administrators who are responsible for operating and maintaining network equipment; consequently, it assumes a basic working knowledge of general switch functions, the Internet Protocol (IP), and Simple Network Management Protocol (SNMP).

Conventions The following conventions are used throughout this guide to show information:

Note: Emphasizes important information or calls your attention to related features or instructions.

Caution: Alerts you to a potential hazard that could cause loss of data, or damage the system or equipment.

Warning: Alerts you to a potential hazard that could cause personal injury.

Related Publications The following publication details the hardware features of the switch, including the physical and performance-related characteristics, and how to install the switch:

The *Installation Guide*

Also, as part of the switch's software, there is an online web-based help that describes all management related features.

Revision History This section summarizes the changes in each revision of this guide.

July 2010 Revision

This is the first version of this guide. This guide is valid for software release v1.1.1.4.

CONTENTS

ABOUT THIS GUIDE 5

CONTENTS 7

FIGURES 11

TABLES 13

SECTION I GETTING STARTED 15

1 INTRODUCTION 17

Key Features 17

Description of Software Features 18

Configuration Backup and Restore 18

Authentication 18

Port Configuration 18

Rate Limiting 18

Port Mirroring 18

Port Trunking 19

Storm Control 19

Static Addresses 19

IEEE 802.1D Bridge 19

Store-and-Forward Switching 19

Spanning Tree Algorithm 19

Virtual LANs 20

Traffic Prioritization 20

Multicast Filtering 20

System Defaults 21

2 INITIAL SWITCH CONFIGURATION 23

Connecting to the Switch 23

Setting an IP Address 23

Setting a Password 25

Changing a PC's IP Address 27

SECTION II WEB CONFIGURATION 29

3 USING THE WEB INTERFACE 31
Connecting to the Web Interface 31
Navigating the Web Browser Interface 32
Home Page 32
Configuration Options 32
Panel Display 33
Main Menu 33

4 SYSTEM SETTINGS 37
Displaying System Information 37
Setting a User Account 39
Setting an IP Address 40
Setting an IPv4 Address 40
Setting an IPv6 Address 41

5 PORT SETTINGS 45

6 LINK AGGREGATION 49
General Link Aggregation Guidelines 49
Creating Trunk Groups 50
Configuring Trunk Settings 52
Configuring LACP 54

7 CREATING VLANS 57
IEEE 802.1Q VLANs 57
Assigning Ports to VLANs 58
Configuring VLAN Attributes for Port Members 60

8 VLAN STACKING 61
Configuring IEEE 802.1Q Tunneling 61
VLAN Stacking Table 62
VLAN Stacking Settings 63

9 IGMP SNOOPING 65
IGMP Snooping Introduction 65

Multicast Entry Table 66
IGMP Snooping Setting 67
IGMP Global Setting 67
IGMP VLAN Setting 69

10 SPANNING TREE 71
Configuring the Spanning Tree Protocol 71
Configuring STP Global Settings 72
Configuring STP Port Settings 75

11 QUALITY OF SERVICE 79
QoS Introduction 79
Port-Based Priority 80
DSCP-Based Priority 81
Priority-to-Queue Mapping 82
Packet Scheduling 84

12 LINK LAYER DISCOVERY PROTOCOL 87
Configuring LLDP 87
LLDP Neighbors 89

13 SNMP SETTINGS 91
Simple Network Management Protocol 91
Setting SNMP System and Community Strings 92
Specifying SNMP Trap Receivers 93

14 PORT MIRRORING 95

15 PORT SECURITY 97

16 BANDWIDTH CONTROL 99

17 JUMBO FRAME 101

18 MANAGEMENT ACCESS FILTER 103

19 MAC ADDRESS SECURITY 105
MAC Forwarding Table 105
Static MAC Addresses 106
MAC Address Filtering 107

20 802.1X SECURITY 109
Configuring 802.1X Authentication 109

802.1X Global Settings 110
802.1X Port Settings 111

21 GENERAL SECURITY SETTINGS 113
IP Filter Security 113
Storm Control Setting 114
Port Isolation 116
Defence Engine 117

22 PORT STATISTICS 119

23 MANAGEMENT TOOLS 121
HTTP Upgrade 121
Restoring Factory Defaults 122
Resetting the Switch 123

SECTION III APPENDICES 125

A SOFTWARE SPECIFICATIONS 127
Software Features 127
Management Features 128
Standards 128
Management Information Bases 129

B TROUBLESHOOTING 131
Problems Accessing the Management Interface 131

GLOSSARY 133

INDEX 139

FIGURES

Figure 1: Login Page 24
Figure 2: Web Interface Home Page 24
Figure 3: IP Settings Page 25
Figure 4: User Accounts Page 26
Figure 5: Home Page 32
Figure 6: Front Panel Indicators 33
Figure 7: System Information 38
Figure 8: System Password 39
Figure 9: IPv4 Address Configuration 41
Figure 10: IPv6 Address Configuration 43
Figure 11: Port Configuration 47
Figure 12: Trunk Group Setting 51
Figure 13: Trunk Distribution Algorithm Setting 53
Figure 14: LACP Port Configuration 55
Figure 15: VLAN Membership Configuration 59
Figure 16: VLAN Port Configuration 60
Figure 17: VLAN Stacking Table 63
Figure 18: VLAN Stacking Settings 64
Figure 19: Multicast Entry Table 67
Figure 20: IGMP Snooping Global Settings 69
Figure 21: IGMP Snooping VLAN Settings 70
Figure 22: STP Global Setting 74
Figure 23: STP Port Setting 78
Figure 24: Port-Based Priority Setting 81
Figure 25: DSCP-Based Priority Setting 82
Figure 26: Priority-to-Queue Mapping 84
Figure 27: Packet Scheduling 85
Figure 28: LLDP Settings 88
Figure 29: LLDP Neighbors 90
Figure 30: SNMP Settings 93
Figure 31: SNMP Trap Receiver Settings 94

Figure 32: Port Mirroring 96
Figure 33: Port Security 98
Figure 34: Bandwidth Control 100
Figure 35: Jumbo Frame Setting 101
Figure 36: Management Access Filter 104
Figure 37: MAC Address Forwarding Table 106
Figure 38: Static MAC Setting 107
Figure 39: MAC Address Filtering 108
Figure 40: 802.1X Setting 111
Figure 41: 802.1X Port Setting 112
Figure 42: IP Filter Setting 114
Figure 43: Storm Control Settings 115
Figure 44: Port Isolation Settings 116
Figure 45: Defence Engine Setting 117
Figure 46: Port Statistics 120
Figure 47: Software Upgrade 122
Figure 48: Restoring Factory Defaults 122
Figure 49: Reboot Switch 123

TABLES

Table 1:	Key Features	17
Table 2:	System Defaults	21
Table 3:	Web Page Configuration Buttons	32
Table 4:	Main Menu	33
Table 5:	Recommended STP Path Cost Range	75
Table 6:	Recommended STP Path Costs	75
Table 7:	Default STP Path Costs	76
Table 8:	Default Mapping of CoS Values to Egress Queues	82
Table 9:	CoS Priority Levels	83
Table 10:	LLDP System Capabilities	89
Table 11:	Troubleshooting Chart	131

SECTION I

GETTING STARTED

This section provides an overview of the switch, and introduces some basic concepts about network switches. It also describes the basic settings required to access the management interface.

This section includes these chapters:

- "Introduction" on page 17
- "Initial Switch Configuration" on page 23

1 INTRODUCTION

This switch provides a broad range of features for Layer 2 switching. It includes a management agent that allows you to configure the features listed in this manual. The default configuration can be used for most of the features provided by this switch. However, there are many options that you should configure to maximize the switch's performance for your particular network environment.

KEY FEATURES

Table 1: Key Features

Feature	Description
Configuration Backup and Restore	Backup to management station or TFTP server
Authentication	Web – user name/password, RADIUS SNMP v1/2c - Community strings Port – IEEE 802.1X, MAC address filtering DHCP Snooping (with Option 82 relay information) IP Filter
DHCP Client	Supported
Port Configuration	Speed, duplex mode, flow control
Rate Limiting	Input rate limiting per port
Port Mirroring	One or more ports mirrored to single analysis port
Port Trunking	Supports up to 8 trunks using either static or dynamic trunking (LACP)
Storm Control	Throttling for broadcast, multicast, and unknown unicast storms
Address Table	Up to 16K MAC addresses in the forwarding table, 1024 static MAC addresses
IP Version 4 and 6	Supports IPv4 and IPv6 addressing
IEEE 802.1D Bridge	Supports dynamic data switching and addresses learning
Store-and-Forward Switching	Supported to ensure wire-speed switching while eliminating bad frames
Spanning Tree Algorithm	Supports Rapid Spanning Tree Protocol (RSTP), which includes STP backward compatible mode
Virtual LANs	Up to 256 using IEEE 802.1Q, port-based, and QinQ VLAN Stacking
Traffic Prioritization	Queue mode and CoS configured by port or DSCP
Multicast Filtering	Supports IGMP snooping and query

DESCRIPTION OF SOFTWARE FEATURES

The switch provides a wide range of advanced performance enhancing features. Flow control eliminates the loss of packets due to bottlenecks caused by port saturation. Storm suppression prevents broadcast, multicast, and unknown unicast traffic storms from engulfing the network. Untagged (port-based) and tagged VLANs provide traffic security and efficient use of network bandwidth. CoS priority queueing ensures the minimum delay for moving real-time multimedia data across the network. While multicast filtering provides support for real-time network applications.

Some of the management features are briefly described below.

CONFIGURATION BACKUP AND RESTORE

You can save the current configuration settings to a file on the management station (using the web interface) and later download this file to restore the switch configuration settings.

AUTHENTICATION

This switch authenticates management access via a web browser. User names and passwords can be configured locally Port-based authentication is also supported via the IEEE 802.1X protocol. This protocol uses Extensible Authentication Protocol over LANs (EAPOL) to request user credentials from the 802.1X client, and then uses the EAP between the switch and the authentication server to verify the client's right to access the network via an authentication server (i.e., RADIUS server).

PORT CONFIGURATION

You can manually configure the speed and duplex mode, and flow control used on specific ports, or use auto-negotiation to detect the connection settings used by the attached device. Use the full-duplex mode on ports whenever possible to double the throughput of switch connections. Flow control should also be enabled to control network traffic during periods of congestion and prevent the loss of packets when port buffer thresholds are exceeded. The switch supports flow control based on the IEEE 802.3x standard (now incorporated in IEEE 802.3-2005).

RATE LIMITING

This feature controls the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

PORT MIRRORING

The switch can unobtrusively mirror traffic from any port to a monitor port. You can then attach a protocol analyzer or RMON probe to this port to perform traffic analysis and verify connection integrity.

PORT TRUNKING

Ports can be combined into an aggregate connection. Trunks can be manually set up or dynamically configured using Link Aggregation Control Protocol (LACP – IEEE 802.3-2005). The additional ports dramatically increase the throughput across any connection, and provide redundancy by taking over the load if a port in the trunk should fail. The switch supports up to 8 trunks.

STORM CONTROL

Broadcast, multicast and unknown unicast storm suppression prevents traffic from overwhelming the network.When enabled on a port, the level of broadcast traffic passing through the port is restricted. If broadcast traffic rises above a pre-defined threshold, it will be throttled until the level falls back beneath the threshold.

STATIC ADDRESSES

A static address can be assigned to a specific interface on this switch. Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table. Static addresses can be used to provide network security by restricting access for a known host to a specific port.

IEEE 802.1D BRIDGE

The switch supports IEEE 802.1D transparent bridging. The address table facilitates data switching by learning addresses, and then filtering or forwarding traffic based on this information. The address table supports up to 16K addresses.

STORE-AND-FORWARD SWITCHING

The switch copies each frame into its memory before forwarding them to another port. This ensures that all frames are a standard Ethernet size and have been verified for accuracy with the cyclic redundancy check (CRC). This prevents bad frames from entering the network and wasting bandwidth.

To avoid dropping frames on congested ports, the switch provides 448 KB for frame buffering. This buffer can queue packets awaiting transmission on congested networks.

SPANNING TREE ALGORITHM

The switch supports these spanning tree protocols:

- Spanning Tree Protocol (STP, IEEE 802.1D) – Supported by using the STP backward compatible mode provided by RSTP. STP provides loop detection. When there are multiple physical paths between segments, this protocol will choose a single path and disable all others to ensure that only one route exists between any two stations on the network. This prevents the creation of network loops. However, if the chosen path should fail for any reason, an alternate path will be activated to maintain the connection.

- Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w) – This protocol reduces the convergence time for network topology changes to about 3 to 5 seconds, compared to 30 seconds or more for the older IEEE 802.1D STP standard. It is intended as a complete replacement for STP, but can still interoperate with switches running the older standard by automatically reconfiguring ports to STP-compliant mode if they detect STP protocol messages from attached devices.

VIRTUAL LANS

The switch supports up to 256 VLANs. A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. The switch supports tagged VLANs based on the IEEE 802.1Q standard. Members of VLAN groups can be manually assigned to a specific set of VLANs. This allows the switch to restrict traffic to the VLAN groups to which a user has been assigned. By segmenting your network into VLANs, you can:

- Eliminate broadcast storms which severely degrade performance in a flat network.
- Simplify network management for node changes/moves by remotely configuring VLAN membership for any port, rather than having to manually change the network connection.
- Provide data security by restricting all traffic to the originating VLAN.

TRAFFIC PRIORITIZATION

This switch prioritizes each packet based on the required level of service, using eight priority queues with strict, Weighted Fair Queuing, or Weighted Round Robin Queuing. It uses IEEE 802.1p and 802.1Q tags to prioritize incoming traffic based on input from the end-station application. These functions can be used to provide independent priorities for delay-sensitive data and best-effort data.

This switch also supports several common methods of prioritizing layer 3/4 traffic to meet application requirements. Traffic can be prioritized based on the priority bits in the IP frame's Type of Service (ToS) octet or the number of the TCP/UDP port. When these services are enabled, the priorities are mapped to a Class of Service value by the switch, and the traffic then sent to the corresponding output queue.

MULTICAST FILTERING

Specific multicast traffic can be assigned to its own VLAN to ensure that it does not interfere with normal network traffic and to guarantee real-time delivery by setting the required priority level for the designated VLAN. The switch uses IGMP Snooping and Query to manage multicast group registration.

SYSTEM DEFAULTS

The following table lists some of the basic system defaults.

Table 2: System Defaults

Function	Parameter	Default
Authentication	User Name	admin
	Password	admin
	802.1X Port Authentication	Disabled
	Port Security	Disabled
	IP Filtering	Disabled
Web Management	HTTP Server	Enabled
	HTTP Port Number	80
SNMP	SNMP Agent	Disabled
	Community Strings	"public" (read only) "private" (read/write)
Port Configuration	Admin Status	Enabled
	Auto-negotiation	Enabled
	Flow Control	Disabled
Rate Limiting	Input and output limits	Disabled
Port Trunking	Static Trunks	None
	LACP (all ports)	Disabled
Storm Protection	Status	Broadcast: disabled Multicast: disabled Unknown unicast: disabled
Spanning Tree Algorithm	Status	Enabled, RSTP (Defaults: RSTP standard)
	Edge Port	Enabled
Virtual LANs	Default VLAN	1
	PVID	1
Traffic Prioritization	Ingress Port Priority	0
	Queue Mode	Weighted Fair Queuing
	Weighted Fair Queuing	Queue: 1 2 3 4 5 6 7 8 Weight: 1 2 3 4 5 6 7 8
	IP DSCP Priority	Disabled
IP Settings	IP Address	192.168.1.1
	Subnet Mask	255.255.255.0
	Default Gateway	0.0.0.0
	DHCP	Client: Disabled
Multicast Filtering	IGMP Snooping	Snooping: Disabled Querier: Disabled

2 INITIAL SWITCH CONFIGURATION

This chapter includes information on connecting to the switch and basic configuration procedures.

The switch includes a built-in network management agent. The agent offers a web-based management interface, and it also supports management through SNMP (Simple Network Management Protocol).

The switch's web management interface allows you to configure switch parameters, monitor port connections, and display statistics using a standard web browser such as Internet Explorer 5.x or above, Netscape 6.2 or above, and Mozilla Firefox 2.0 or above. The web management interface can be accessed from any computer attached to the network.

CONNECTING TO THE SWITCH

To make use of the management features of your switch, you must first configure it with an IP address that is compatible with the network it is being installed in. This should be done before you permanently install the switch in the network.

NOTE: By default, the IPv4 address for this switch is set to 192.168.1.1 with subnet mask 255.255.255.0.

SETTING AN IP ADDRESS

Follow this procedure:

1. Place your switch close to the PC that you intend to use for configuration. It helps if you can see the front panel of the switch while working on your PC.

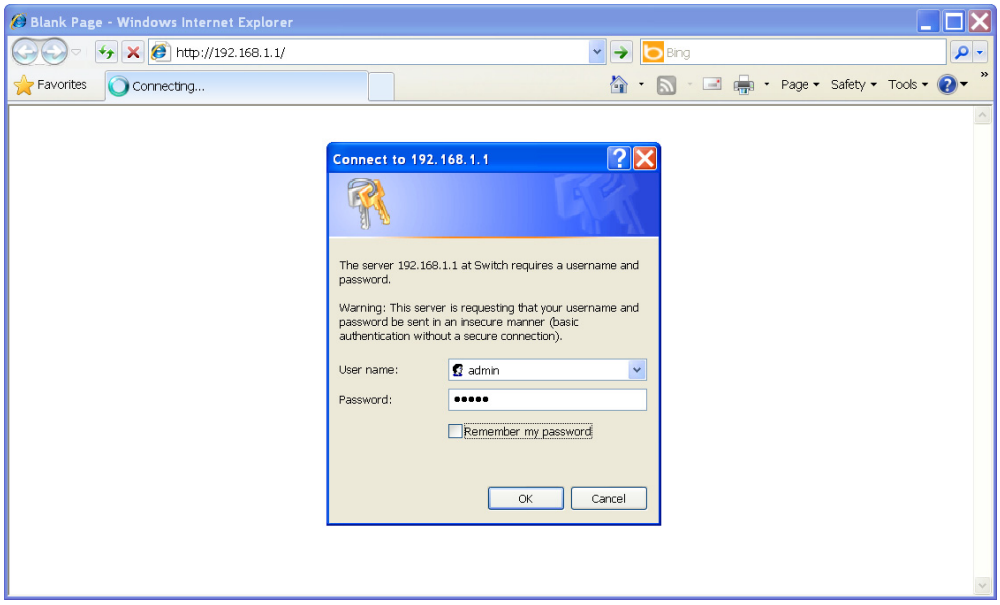
2. Connect the Ethernet port of your PC to any port on the front panel of your switch. Connect power to the switch and verify that you have a link by checking the front-panel LEDs.

3. Check that your PC has an IP address on the same subnet as the switch. The default IP address of the switch is 192.168.1.1 and the subnet mask is 255.255.255.0, so the PC and switch are on the same subnet if they both have addresses that start 192.168.1.x. If the PC and switch are not on the same subnet, you must manually set the PC's IP address to 192.168.1.x (where "x" is any number from 2 to 255). If

you are unfamiliar with this process, see "Changing a PC's IP Address" on page 27.

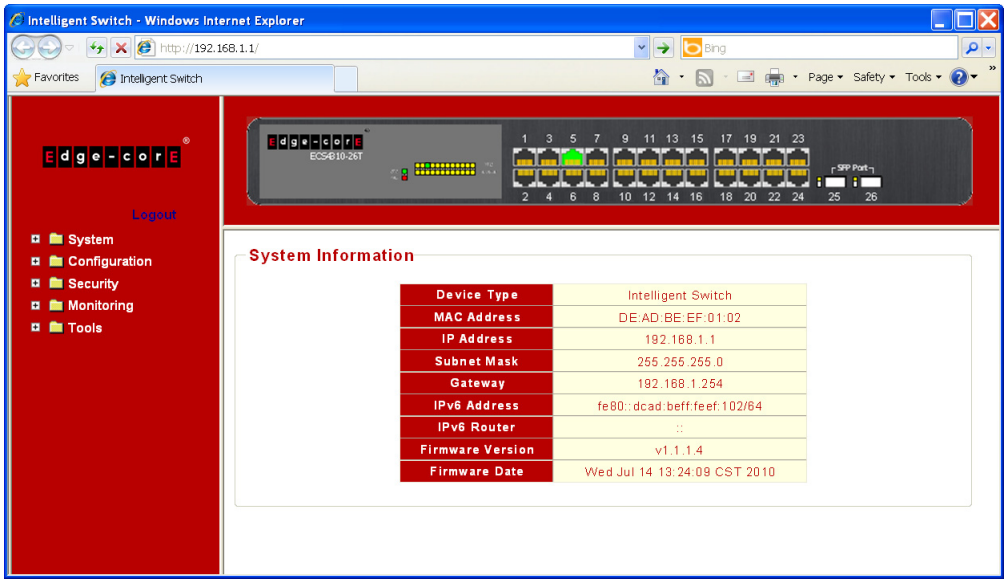
4. Open your web browser and enter the address http://192.168.1.1. If your PC is properly configured, you will see the login page of your switch. If you do not see the login page, repeat step 3.

Figure 1: Login Page



5. Enter the default user name "admin" and password "admin," then click the OK button to access the web interface home page.

Figure 2: Web Interface Home Page

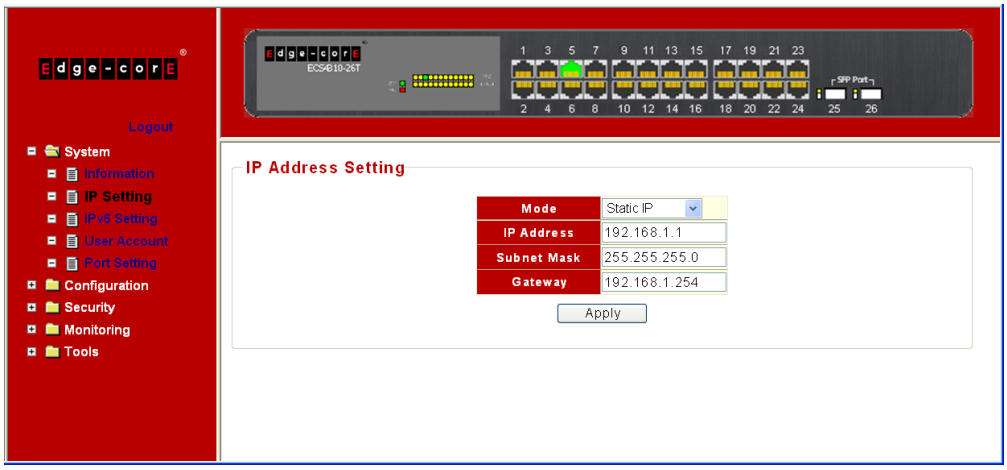


6. From the menu, click on System, then IP Settings. On the IP Address Setting page, enter the new IP address, Subnet Mask and Gateway IP Address for the switch, then click on the Apply button.

NOTE: The switch also supports dynamic IPv4 address assignment through DHCP (Dynamic Host Configuration Protocol). The switch sends IPv4 configuration requests to DHCP servers on the network.

NOTE: The switch also supports IPv6 addressing. By default the switch automatically generates a unique IPv6 host address based on the local subnet address prefix received in router advertisement messages. For more information, see "Setting an IPv6 Address" on page 41.

Figure 3: IP Settings Page



SETTING A PASSWORD

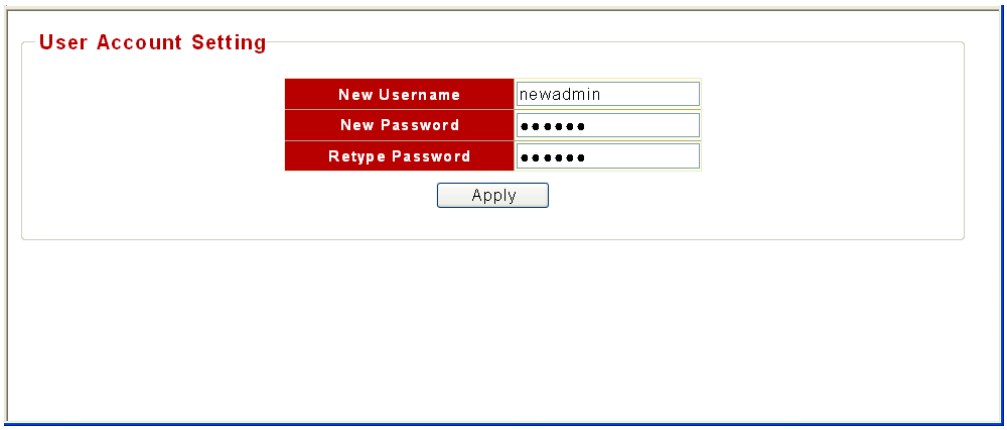
No other configuration changes are required at this stage, but before logging out it is recommended that you change the default administrator's user name and password for access to the switch, record them, and put them in a safe place.

User names can consist of up to 16 alphanumeric characters, and passwords can be up to 8 characters. Both user names and passwords are case sensitive.

To prevent unauthorized access to the switch, set a password as follows:

1. On the menu, click System and then User Account.

Figure 4: User Accounts Page



2. In the New Username field, define an administrator user name.
3. In the New Password field, define an administrator password.
4. Confirm the new password setting in the Retype Password field.
5. Click the Apply button.

CHANGING A PC'S IP ADDRESS

To change the IP address of a Windows 2000 PC:

1. Click Start, Settings, then Network and Dial-up Connections.
2. For the IP address you want to change, right-click the network connection icon, and then click Properties.
3. In the list of components used by this connection on General tab, select Internet Protocol (TCP/IP), and then click the Properties button.
4. In the Internet Protocol (TCP/IP) Properties dialog box, click to select Use the following IP address. Then type your intended IP address, Subnet mask, and Default gateway in the provided text boxes.
5. Click OK to save the changes.

To change the IP address of a Windows XP PC:

1. Click Start, Control Panel, then Network Connections.
2. For the IP address you want to change, right-click the network connection icon, and then click Properties.
3. In the list of components used by this connection on General tab, select Internet Protocol (TCP/IP), and then click the Properties button.
4. In the Internet Protocol (TCP/IP) Properties dialog box, click to select Use the following IP address. Then type your intended IP address, Subnet mask, and Default gateway in the provided text boxes
5. Click OK to save the changes.

NOTE: For users of systems other than Windows 2000 or Windows XP, refer to your system documentation for information on changing the PC's IP address.

SECTION II

WEB CONFIGURATION

This section describes the basic switch features, along with a detailed description of how to configure each feature via a web browser.

This section includes these chapters:

- "Using the Web Interface" on page 31
- "System Settings" on page 37
- "Port Settings" on page 45
- "Link Aggregation" on page 49
- "Creating VLANs" on page 57
- "VLAN Stacking" on page 61
- "IGMP Snooping" on page 65
- "Spanning Tree" on page 71
- "Quality of Service" on page 79
- "Link Layer Discovery Protocol" on page 87
- "SNMP Settings" on page 91
- "Port Mirroring" on page 95
- "Port Security" on page 97
- "Bandwidth Control" on page 99
- "Jumbo Frame" on page 101
- "Management Access Filter" on page 103
- "MAC Address Security" on page 105
- "802.1X Security" on page 109

- "General Security Settings" on page 113
- "Port Statistics" on page 119
- "Management Tools" on page 121

3 USING THE WEB INTERFACE

The switch provides an embedded HTTP web agent. Using a web browser you can configure the switch and view statistics to monitor network activity. The web agent can be accessed by any computer on the network using a standard web browser (Internet Explorer 5.0, Netscape 6.2, Mozilla Firefox 2.0, or more recent versions).

CONNECTING TO THE WEB INTERFACE

Prior to accessing the switch from a web browser, be sure you have first performed the following tasks:

1. Configured the switch with a valid IP address, subnet mask, and default gateway using the web interface, or DHCP protocol. By default, the IPv4 address is set to 192.168.1.1. (See "Setting an IP Address" on page 40.)

2. Set the system password using the web interface. (See "Setting a User Account" on page 39.)

3. After you enter a user name and password, you will have access to the system configuration program.

NOTE: You are allowed three attempts to enter the correct password; on the third failed attempt the current connection is terminated.

NOTE: If the path between your management station and this switch does not pass through any device that uses the Spanning Tree Protocol, then you can set the switch port attached to your management station to fast forwarding (enable as an Edge port) to improve the switch's response time to management commands issued through the web interface. See "Configuring STP Port Settings" on page 75.

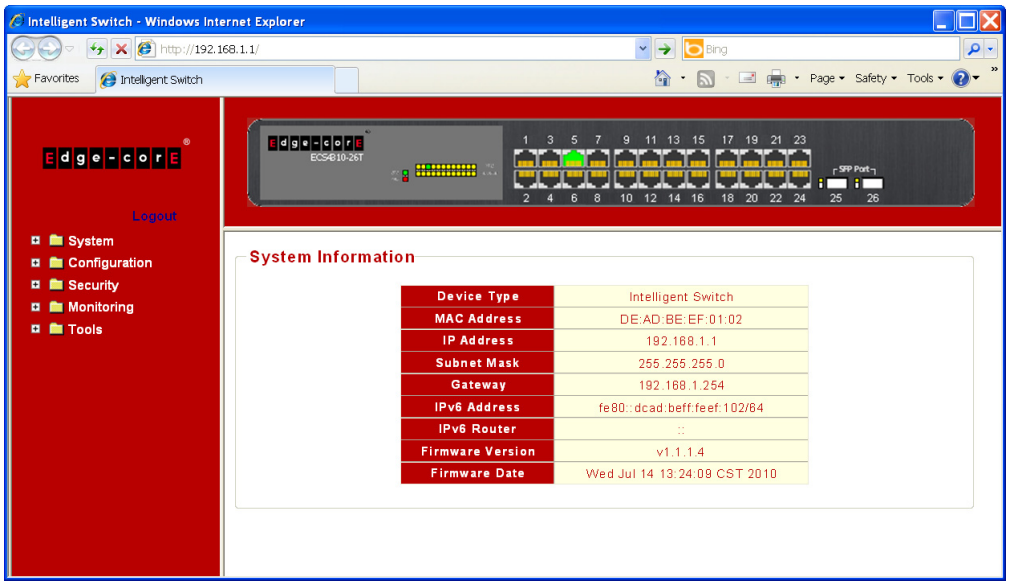
NAVIGATING THE WEB BROWSER INTERFACE

To access the web-browser interface you must first enter a user name and password. By default, the user name is "admin" and password "admin."

HOME PAGE

When your web browser connects with the switch's web agent, the home page is displayed as shown below. The home page displays the Main Menu on the left side of the screen and an image of the front panel on the right side. The Main Menu links are used to navigate to other menus, and display configuration parameters and statistics.

Figure 5: Home Page



CONFIGURATION OPTIONS

Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a page, be sure to click on the Apply button to confirm the new setting. The following table summarizes common web page configuration buttons.

Table 3: Web Page Configuration Buttons

Button	Action
Apply	Sets specified values to the system.
Add	Adds an entry to a feature table.
Delete	Removes an entry from a feature table.

NOTE: To ensure proper screen refresh, be sure that Internet Explorer is configured so that the setting "Check for newer versions of stored pages" reads "Every visit to the page."

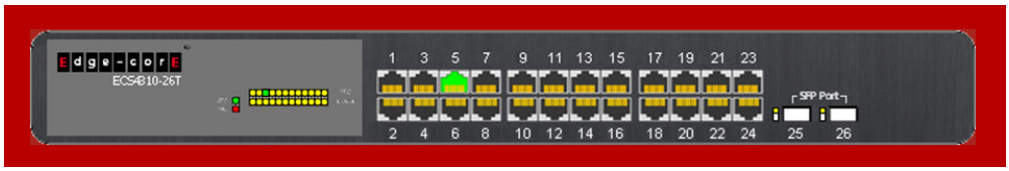
Internet Explorer 6.x and earlier: This option is available under the menu "Tools / Internet Options / General / Temporary Internet Files / Settings."

Internet Explorer 7.x: This option is available under "Tools / Internet Options / General / Browsing History / Settings / Temporary Internet Files."

PANEL DISPLAY

The web agent displays an image of the switch's ports. The data displayed on the screen is automatically refreshed approximately once every 10 seconds.

Figure 6: Front Panel Indicators



MAIN MENU

Using the onboard web agent, you can define system parameters, manage and control the switch, and all its ports, or monitor network conditions. The following table briefly describes the selections available from this program.

Table 4: Main Menu

Menu	Description	Page
System		
Information	Configures system contact, name and location	37
IP Setting	Configures IPv4 settings	40
IPv6 Setting	Configures IPv6 settings	41
User Account	Configures system password	39
Port Settings	Configures port connection settings	45
Configuration		
Link Aggregation		
Trunk Group Setting	Specifies ports to group into static trunks	50
Trunk Setting	Configures the trunk balancing algorithm	52
LACP Setting	Allows ports to dynamically join trunks	54
VLAN		
Static VLAN	Configures VLAN groups	58
VLAN Setting	Specifies default PVID for ports	60

Table 4: Main Menu

Menu	Description	Page
VLAN Stacking		
S-VLAN Table	Sets QinQ settings for the switch	62
S-VLAN Setting	Sets QinQ settings for ports	63
IGMP Snooping		
Multicast Entry Table	Displays multicast groups to be filtered for VLANs	66
IGMP Snooping Setting	Configures global and port settings for multicast filtering	67
Spanning Tree		
STP Global Setting	Configures global bridge settings for RSTP	72
STP Port Setting	Configures individual port settings for RSTP	75
QoS		
Port-based Priority	Configures the default CoS traffic class for ports	80
DSCP-based Priority	Maps DSCP values to standard CoS classes	81
Priority to Queue Mapping	Configures CoS traffic class to port queue mapping	82
Packet Scheduling	Configures port queue mode and queue weights	84
LLDP		
LLDP-Setting	Configures global and port LLDP settings	87
LLDP Neighbors	Displays LLDP information about a remote device connected to ports on this switch	89
SNMP	Configures read-only and read/write community strings for SNMP v1/v2c, engine ID for SNMP v3, and trap parameters	91
Port Mirroring	Sets source and target ports for mirroring	95
Port Security	Configures source MAC address limits for ports	97
Bandwidth Control	Configures ingress and egress rate limits	99
Jumbo Frame	Enables Jumbo Frame support	101
Management Access Filter	Sets IP addresses of clients allowed management access	103
Security		
MAC Address		
MAC Forwarding Table	Displays dynamic and static addresses	105
Static MAC	Configures static MAC addresses	106
MAC Filtering	Sets source and destination MAC address filters	107
802.1x		
802.1x Setting	Configures global 802.1X settings	110
802.1x Port Setting	Configures 802.1X settings for ports	111
IP Filter Setting	Filters traffic based IP addresses	113
Storm Control	Sets limits for broadcast, multicast, and unknown unicast traffic	114

Table 4: Main Menu

Menu	Description	Page
Port Isolation	Limits traffic to and from specified ports	116
Defence Engine	Provides protection from traffic storms	117
Monitoring		
Port Statistics	Shows detailed Ethernet port statistics	119
Tools		
HTTP Upgrade	Updates software on the switch, and saves/restores configuration settings from a file on the management station	121
Reset	Restarts the switch and restores factory default settings	122
Reboot	Restarts the switch	123

4 SYSTEM SETTINGS

This chapter describes some basic system settings on the switch. It includes the following sections:

- "Displaying System Information" on page 37
- "Setting a User Account" on page 39
- "Setting an IP Address" on page 40

DISPLAYING SYSTEM INFORMATION

The System>Information page displays some basic settings for the switch, including MAC address, IPv4 and IPv6 settings, and software version information.

PARAMETERS

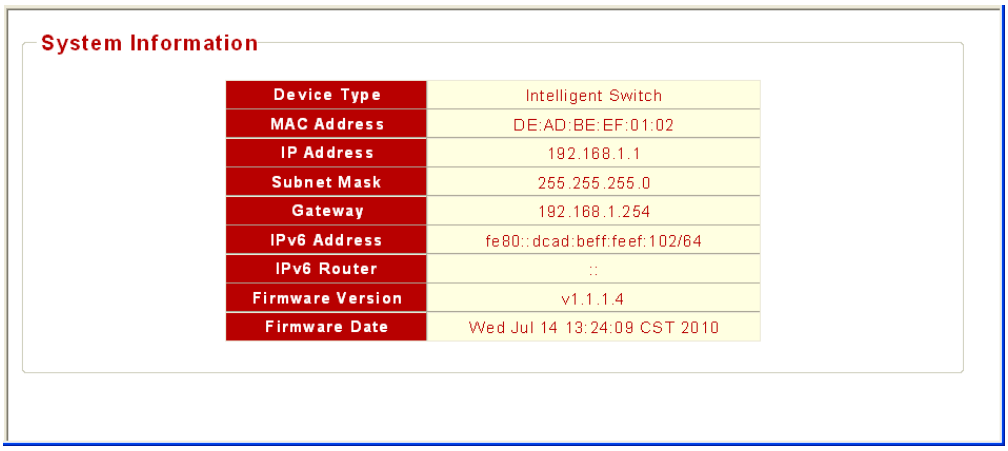
These parameters are displayed on the System Information page:

- **Device Type** – Describes the switch system type.
- **MAC Address** – The physical layer address for this switch.
- **IP Address** – The current IPv4 address of the switch.
- **Subnet Mask** – The current IPv4 subnet mask of the switch.
- **Gateway** – IPv4 address of the gateway router between the switch and management stations that exist on other network segments.
- **IPv6 Address** – The current IPv6 address of the switch.
- **IPv6 Router** – The IPv6 address of the default next hop router.
- **Firmware Version** – Version number of the switch software.
- **Firmware Date** – Release date of the switch software.

WEB INTERFACE

To view System Information in the web interface, click System, then Information.

Figure 7: System Information



SETTING A USER ACCOUNT

The administrator has read/write access for all parameters governing the onboard agent. You should therefore assign a new administrator user name and password as soon as possible, and store them in a safe place.

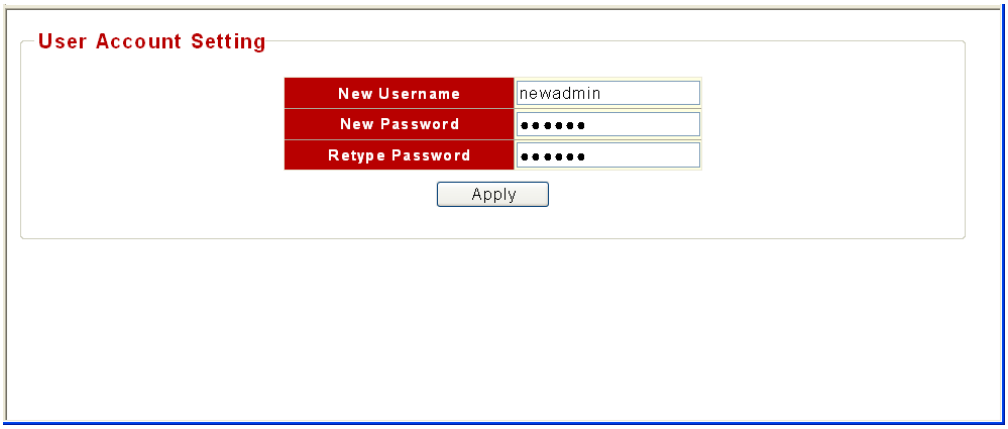
The default administrator user name is "admin" and password is "admin." User names can consist of up to 16 alphanumeric characters, and passwords can be up to 8 characters. Both user names and passwords are case sensitive.

WEB INTERFACE

To configure the System Password in the web interface:

1. Click System, then User Account.
2. Enter the new user name.
3. Enter the new password.
4. Enter the new password again to confirm your input.
5. Click Save.

Figure 8: System Password



SETTING AN IP ADDRESS

This section describes how to configure an IP interface for management access to the switch over the network. This switch supports both IP Version 4 and Version 6, and can be managed simultaneously through either of these address types. You can manually configure a specific IPv4 or IPv6 address, or direct the switch to obtain an IPv4 address from a DHCP server when it is powered on. An IPv6 address can either be manually configured or automatically generated.

SETTING AN IPV4 ADDRESS

The IPv4 address for the switch is set to 192.168.1.1 by default. You may need to manually configure the switch's default settings to values that are compatible with your network. You may also need to a establish a default gateway between the switch and management stations that exist on another network segment.

You can manually configure a specific IPv4 address, or direct the device to obtain an address from a DHCP server. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything other than this format will not be accepted by the CLI program.

PARAMETERS

The following parameters are displayed on the IP Address Setting page:

- **Mode** – Specifies whether IP settings are assigned manually or through the Dynamic Host Configuration Protocol (DHCP). (Default: Static IP)
  - **Static IP** – The IPv4 settings are set manually by the user.
  - **DHCP** – When enabled, IP will not function until a reply has been received from the server. Requests will be broadcast periodically by the switch for an IP address. DHCP values can include the IP address, subnet mask, and default gateway.

NOTE: If the switch does not receive a response from a DHCP server, it will have no configured IPv4 address.

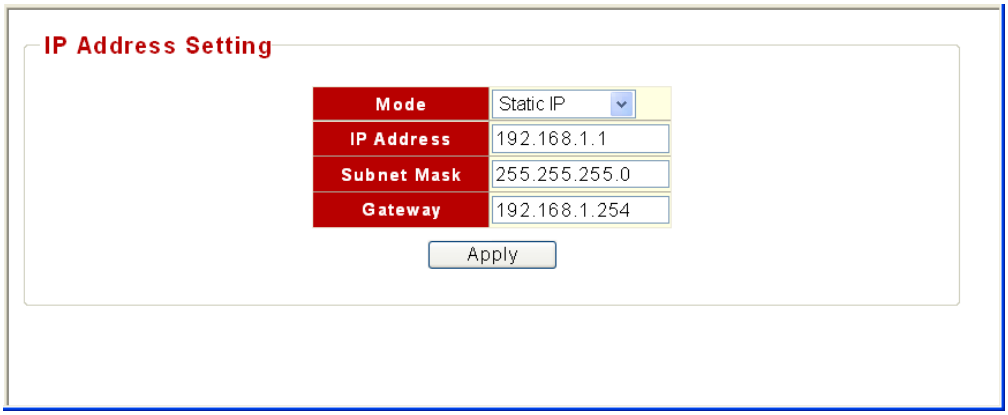
- **IP Address** – The IPv4 address for the switch. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. (Default: 192.168.1.1)
- **IP Mask** – This mask identifies the host address bits used for routing to specific subnets. (Default: 255.255.255.0)
- **IP Router** – IP address of the gateway router between the switch and management stations that exist on other network segments.

WEB INTERFACE

To configure static IPv4 address settings:

1. Click System, then IP Setting.
2. Set the Mode to "Static IP."
3. Specify the IPv4 address, subnet mask, and gateway address.
4. Click Apply.

Figure 9: IPv4 Address Configuration



SETTING AN IPV6 ADDRESS

This section describes how to configure an IPv6 interface for management access over the network.

IPv6 includes two distinct address types; link-local unicast and global unicast. A link-local address makes the switch accessible over IPv6 for all devices attached to the same local subnet. Management traffic using this kind of address cannot be passed by any router outside of the subnet. A link-local address is easy to set up, and may be useful for simple networks or basic troubleshooting tasks. However, to connect to a larger network with multiple segments, the switch must be configured with a global unicast address. A link-local address must be manually configured, but a global unicast address can either be manually configured or dynamically assigned.

USAGE GUIDELINES

- All IPv6 addresses must be formatted according to RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill the undefined fields.
- When configuring a link-local address, note that the prefix length is fixed at 64 bits, and the host portion of the default address is based on the modified EUI-64 (Extended Universal Identifier) form of the

interface identifier (i.e., the physical MAC address). You can manually configure a link-local address by entering the full address with the network prefix FE80.

- To connect to a larger network with multiple subnets, you must configure a global unicast address. There are several alternatives to configuring this address type:
  - The global unicast address can be automatically configured by taking the network prefix from router advertisements observed on the local interface, and using the modified EUI-64 form of the interface identifier to automatically create the host portion of the address. This option can be selected by enabling the Auto Configuration option.
  - You can also manually configure the global unicast address by entering the full address and prefix length.

PARAMETERS

The following parameters are displayed on the IPv6 Address Setting page:

- **Auto Configuration** – Enables stateless autoconfiguration of IPv6 addresses on an interface and enables IPv6 functionality on the interface. The network portion of the address is based on prefixes received in IPv6 router advertisement messages, and the host portion is automatically generated using the modified EUI-64 form of the interface identifier; i.e., the switch's MAC address. (Default: Disabled)
- **IPv6 Address** – Manually configures a global unicast address by specifying the full address and network prefix length (in the Prefix field). (Default: *null*)
- **Prefix Length** – Defines the prefix length as a decimal value indicating how many contiguous bits (starting at the left) of the address comprise the prefix; that is, the network portion of the address. (Default: 0)
- **Router** – Sets the IPv6 address of the default next hop router.

  An IPv6 default gateway must be defined if the management station is located in a different IPv6 segment.

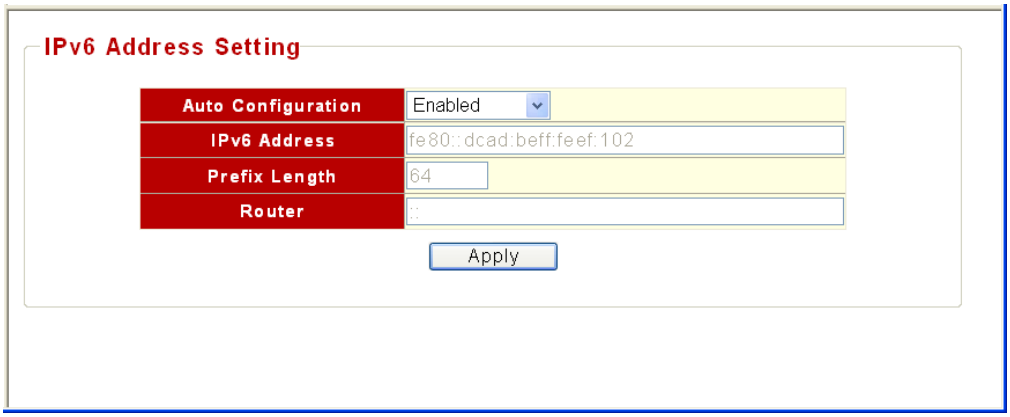
  An IPv6 default gateway can only be successfully set when a network interface that directly connects to the gateway has been configured on the switch.

WEB INTERFACE

To configure IPv6 & Time in the web interface:

1. Click Configuration, System, IPv6 & Time.
2. Specify the IPv6 settings, and indicate the local time zone by configuring the appropriate offset. The information shown below provides a example of how to manually configure an IPv6 address.
3. Click Save.

Figure 10: IPv6 Address Configuration



5 PORT SETTINGS

The Port Configuration page includes configuration options for enabling auto-negotiation or manually setting the speed and duplex mode, or enabling flow control.

PARAMETERS

The following parameters are displayed on the Port Configuration page:

- **Port** – Selects one or more ports or trunks to configure. Hold down the Ctrl key and click port numbers to selelct multiple ports. Hold down the Shift key to select a range of ports.
- **State** – Sets the link state of port interfaces. (Default: Enabled)
  - **Enable** - Enables port interfaces.
  - **Disable** - Disables the interface. You can disable an interface due to abnormal behavior (e.g., excessive collisions), and then re-enable it after the problem has been resolved. You may also disable an interface for security reasons.
- **Speed/Duplex** – Sets the port speed and duplex mode using auto-negotiation or manual selection. (Default: Auto-negotiation enabled)
  - **Auto** - Enables auto-negotiation. When using auto-negotiation, the optimal settings will be negotiated between the link partners based on their advertised capabilities. Auto must be enabled for all 1 Gbps connections.
  - **100M/Full** - Supports 100 Mbps full-duplex operation
  - **100M/Half** - Supports 100 Mbps half-duplex operation
  - **10M/Full** - Supports 10 Mbps full-duplex operation
  - **10M/Half** - Supports 10 Mbps half-duplex operation

NOTE: The 1000BASE-T standard does not support forced mode. Auto-negotiation should always be used to establish a connection over any 1000BASE-T port or trunk. If not used, the success of the link process cannot be guaranteed when connecting to other types of switches.

- **Flow Control** – Flow control can eliminate frame loss by "blocking" traffic from end stations or segments connected directly to the switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3-2005 (formally IEEE 802.3x) for full-duplex operation. (Default: Enabled)

NOTE: Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub.

Current Port Status

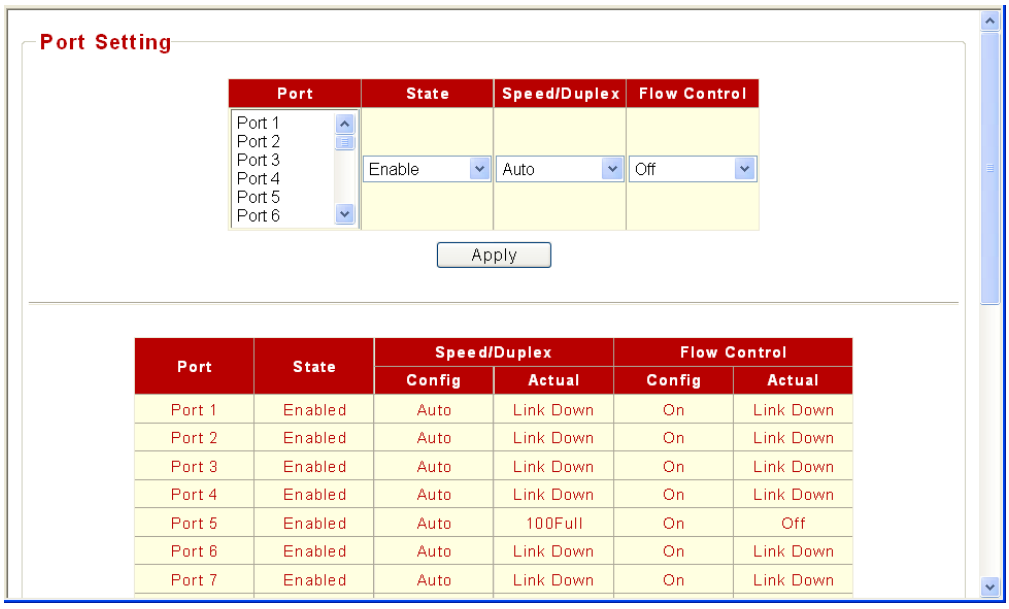
- **Port** – The number of the port or trunk interface.
- **State** – Indicates if the port is enabled or disabled.
- **Speed/Duplex** – Displays the following:
  - **Config** – The configured speed/duplex mode of the port.
  - **Actual** – Indicates the link status of the port. When a link is up, indicates the operating speed and duplex mode.
- **Flow Control** – Displays the following:
  - **Config** – The configured flow control mode of the port.
  - **Actual** – Indicates the link status of the port. When a link is up, indicates the operating flow control mode.

WEB INTERFACE

To configure port connection settings in the web interface:

1. Click System, Port Setting.
2. Select one or more ports or trunks to configure.
3. Make any required changes to the connection settings.
4. Click Apply.

Figure 11: Port Configuration



6 LINK AGGREGATION

You can create multiple links between devices that work as one virtual, aggregate link. A port trunk offers a dramatic increase in bandwidth for network segments where bottlenecks exist, as well as providing a fault-tolerant link between two switches.

This chapter includes the following sections for configuring link aggregation:

- "General Link Aggregation Guidelines" on page 49
- "Creating Trunk Groups" on page 50
- "Configuring Trunk Settings" on page 52
- "Configuring LACP" on page 54

GENERAL LINK AGGREGATION GUIDELINES

The switch supports both static trunking and dynamic Link Aggregation Control Protocol (LACP). Static trunks have to be manually configured at both ends of the link, and the switches must comply with the Cisco EtherChannel standard. On the other hand, LACP configured ports can automatically negotiate a trunked link with LACP-configured ports on another device. You can configure any number of ports on the switch to use LACP, as long as they are not already configured as part of a static trunk. If ports on another device are also configured to use LACP, the switch and the other device will negotiate a trunk between them. If an LACP trunk consists of more than eight ports, all other ports will be placed in standby mode. Should one link in the trunk fail, one of the standby ports will automatically be activated to replace it.

Besides balancing the load across each port in the trunk, the other ports provide redundancy by taking over the load if a port in the trunk fails. However, before making any physical connections between devices, configure the trunk on the devices at both ends. When using a port trunk, take note of the following points:

- Finish configuring port trunks before you connect the corresponding network cables between switches to avoid creating a loop.
- You can create up to 8 trunks on a switch, with up to 8 ports per trunk.
- The ports at both ends of a connection must be configured as trunk ports.

- When configuring static trunks on switches of different types, they must be compatible with the Cisco EtherChannel standard.
- The ports at both ends of a trunk must be configured in an identical manner, including communication mode (that is, speed, duplex mode and flow control), VLAN assignments, and CoS settings.
- Any of the ports on the front panel can be trunked together, including ports of different media types.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- STP, VLAN, and IGMP settings can only be made for the entire trunk.

CREATING TRUNK GROUPS

Use the Trunk Group Setting page to configure the aggregation type and members of each trunk group.

USAGE GUIDELINES

- When configuring static trunks, you may not be able to link switches of different types, depending on the manufacturer's implementation. However, note that the static trunks on this switch are Cisco EtherChannel compatible.
- To avoid creating a loop in the network, be sure you add a static trunk using the configuration interface before connecting the ports, and also disconnect the ports before removing a static trunk through the configuration interface.
- Trunk Group Settings also apply to LACP (see "Configuring LACP" on page 54).

PARAMETERS

The following parameters are displayed on the configuration page for Trunk Groups:

- **Group ID** – Trunk identifier. (Range: Trunk1-Trunk8)
- **Type** – Selects the trunk type; Static or LACP.
- **Ports** – Selects one or more ports to configure as a trunk. Hold down the Ctrl key and click port numbers to selelct multiple ports. Hold down the Shift key to select a range of ports. (Range: 1-26)
- **LACP Active** – Indicates ports in an LACP trunk that are members of an active link.

Current Configured Trunk Groups

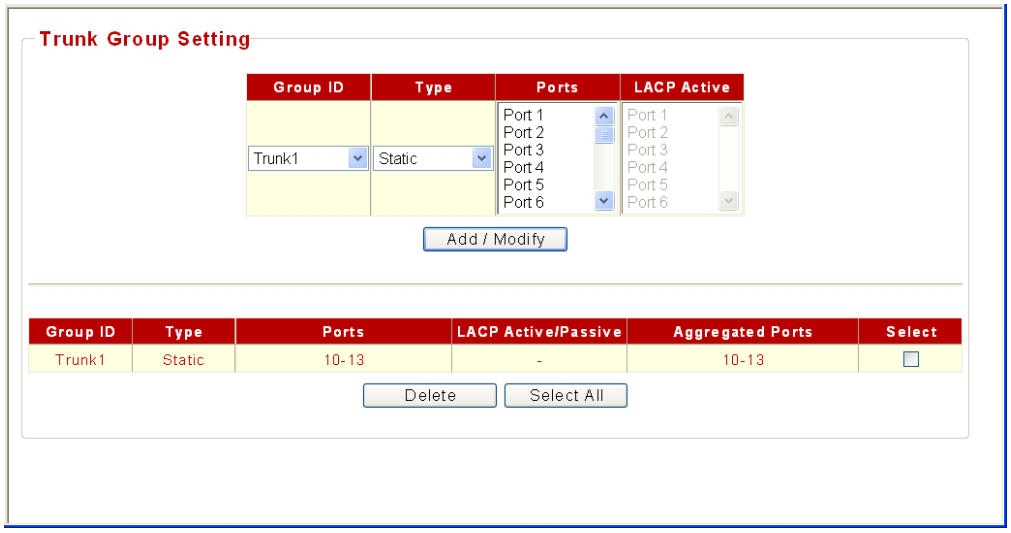
- **Group ID** – Displays the trunk identifier.
- **Type** – Displays the trunk type; Static or LACP.
- **Ports** – Configured port members in the trunk.
- **LACP Active/Passive** – Configured port members in an LACP trunk.
- **Aggregated Ports** – Indicates ports in a trunk that are members of an active link.
- **Select** – Selects a configured trunk to be deleted.

WEB INTERFACE

To configure a trunk group:

1. Click Configuration, Aggregation Link, Trunk Group Setting.
2. Select the trunk group ID to be created or modified.
3. Selec the trunk type; Static or LACP.
4. Assign up to eight port members to the trunk.
5. Click Add/Modify.

Figure 12: Trunk Group Setting



CONFIGURING TRUNK SETTINGS

When incoming data frames are forwarded through the switch to a trunk, the switch must determine to which port link in the trunk an outgoing frame should be sent. To maintain the frame sequence of various traffic flows between devices in the network, the switch also needs to ensure that frames in each "conversation" are mapped to the same trunk link.

To achieve this requirement and to distribute a balanced load across all links in a trunk, the switch uses a hash algorithm to calculate an output link number in the trunk. However, depending on the device to which a trunk is connected and the traffic flows in the network, this load-balance algorithm may result in traffic being distributed mostly on one port in a trunk. To ensure that the switch traffic load is distributed evenly across all links in a trunk, the hash methods used in the load-balance calculation can be selected to provide the best result for trunk connections. The switch provides five load-balancing methods as described below.

PARAMETERS

The following parameters are displayed on the Trunk Setting page:

- **Distribution Algorithm Parameters** – Selects the load-balance method to apply to all trunks on the switch. If more than one option is selected, each factor is used in the hash algorithm to determine the port member within the trunk to which a frame will be assigned. The following options are supported:
  - **Source Port** – All traffic with the same source and destination TCP/UDP port number is output on the same link in a trunk. Avoid using his mode as a lone option. It may overload a single port member of the trunk for application traffic of a specific type, such as web browsing. However, it can be used effectively in combination with the IP Address option.
  - **Source MAC** – All traffic with the same source MAC address is output on the same link in a trunk. This mode works best for switch-to-switch trunk links where traffic through the switch is received from many different hosts. (The default.)
  - **Dest. MAC** – All traffic with the same destination MAC address is output on the same link in a trunk. This mode works best for switch-to-switch trunk links where traffic through the switch is destined for many different hosts. Do not use this mode for switch-to-router trunk links where the destination MAC address is the same for all traffic.
  - **Source IP** – All traffic with the same source and destination IP address is output on the same link in a trunk. This mode works best for switch-to-router trunk links where traffic through the switch is destined for many different hosts. Do not use this mode for switch-to-server trunk links where the destination IP address is the same for all traffic.

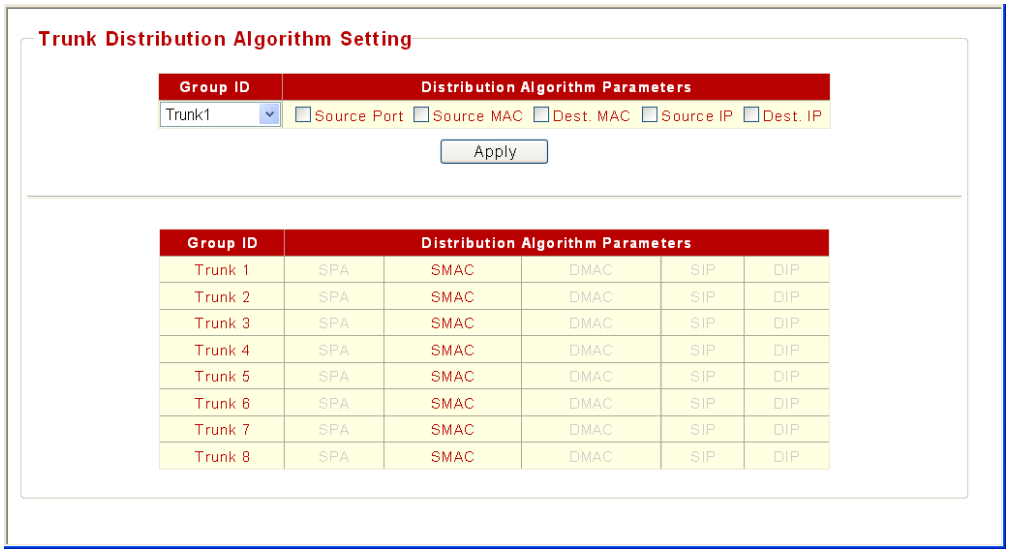
- **Dest. IP** – All traffic with the same source and destination IP address is output on the same link in a trunk. This mode works best for switch-to-router trunk links where traffic through the switch is destined for many different hosts. Do not use this mode for switch-to-server trunk links where the destination IP address is the same for all traffic.

WEB INTERFACE

To configure a trunk's load-balancing settings:

1. Click Configuration, Aggregation Link, Trunk Setting.
2. Select the trunk group ID to be configured or modified.
3. Selec the trunk Distribution Algorithm Parameters as required.
4. Click Apply.

Figure 13: Trunk Distribution Algorithm Setting


Trunk Distribution Algorithm Setting
Group ID
Distribution Algorithm Parameters
Trunk1
Source Port
Source MAC
Dest. MAC
Source IP
Dest. IP
Apply
Group ID
Distribution Algorithm Parameters
Trunk 1 SPA SMAC DMAC SIP DIP
Trunk 2 SPA SMAC DMAC SIP DIP
Trunk 3 SPA SMAC DMAC SIP DIP
Trunk 4 SPA SMAC DMAC SIP DIP
Trunk 5 SPA SMAC DMAC SIP DIP
Trunk 6 SPA SMAC DMAC SIP DIP
Trunk 7 SPA SMAC DMAC SIP DIP
Trunk 8 SPA SMAC DMAC SIP DIP

CONFIGURING LACP

Use the LACP Settings page to enable LACP on the switch and configure the system priority.

USAGE GUIDELINES

- To avoid creating a loop in the network, be sure you enable LACP before connecting the ports, and also disconnect the ports before disabling LACP.
- If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.
- If more than eight ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.
- All ports on both ends of an LACP trunk must be configured for full duplex, either by forced mode or auto-negotiation.
- Trunks dynamically established through LACP will be shown on the Trunk Group Setting page (page 50).
- Ports assigned to a common link aggregation group (LAG) must meet the following criteria:
  - Ports must have the same LACP Admin Key. Using auto-configuration of the Admin Key will avoid this problem.
  - One of the ports at either the near end or far end must be set to active initiation mode.
- The Distribution Algorithm Parameters configured on the Trunk Settings page (see "Configuring Trunk Settings" on page 52) also applies to LACP.

PARAMETERS

The following parameters are displayed on the configuration page for dynamic trunks:

- **LACP Status** – Controls whether LACP is enabled on the switch. LACP will form an aggregation when two or more ports are connected to the same partner. LACP can form up to 8 trunks per switch.
- **System Priority** – LACP system priority is used to determine link aggregation group (LAG) membership, and to identify this device to other switches during LAG negotiations. (Range: 0-65535; Default: 32768)

Current LACP Port Configuration

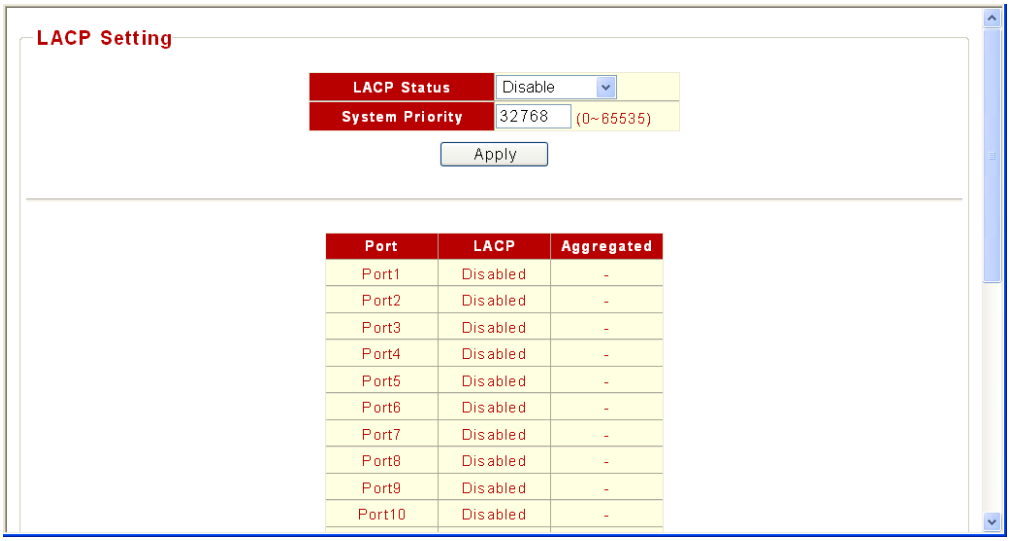
- **Port** – Port identifier. (Range: 1-26)
- **LACP** – Indicates ports that are enabled as LACP ports and if they are passive or active.
- **Aggregated** – Indicates ports in a trunk that are members of an active link.

WEB INTERFACE

To configure LACP settings:

1. Click Configuration, Link Aggregation, LACP Setting.
2. Enable LACP on the switch.
3. Specify the LACP System Priority to identify LAGs on the switch.
4. Click Apply.

Figure 14: LACP Port Configuration



7 CREATING VLANS

This chapter includes the following sections for configuring VLANs:

- "IEEE 802.1Q VLANs" on page 57
- "Assigning Ports to VLANs" on page 58
- "Configuring VLAN Attributes for Port Members" on page 60

IEEE 802.1Q VLANs

In large networks, routers are used to isolate broadcast traffic for each subnet into separate domains. This switch provides a similar service at Layer 2 by using VLANs to organize any group of network nodes into separate broadcast domains. VLANs confine broadcast traffic to the originating group, and can eliminate broadcast storms in large networks. This also provides a more secure and cleaner network environment.

An IEEE 802.1Q VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment.

VLANs help to simplify network management by allowing you to move devices to a new VLAN without having to change any physical connections. VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as e-mail), or multicast groups (used for multimedia applications such as videoconferencing).

VLANs provide greater network efficiency by reducing broadcast traffic, and allow you to make network changes without having to update IP addresses or IP subnets. VLANs inherently provide a high level of network security since traffic must pass through a configured Layer 3 link to reach a different VLAN.

This switch supports the following VLAN features:

- Up to 256 VLANs based on the IEEE 802.1Q standard
- Distributed VLAN learning across multiple switches using explicit or implicit tagging
- Port overlapping, allowing a port to participate in multiple VLANs
- End stations can belong to multiple VLANs
- Passing traffic between VLAN-aware and VLAN-unaware devices
- Priority tagging

ASSIGNING PORTS TO VLANS

Before enabling VLANs for the switch, you must first assign each port to the VLAN group(s) in which it will participate. By default all ports are assigned to VLAN 1 as untagged ports. Add a port as a tagged port if you want it to carry traffic for one or more VLANs, and any intermediate network devices or the host at the other end of the connection supports VLANs. Then assign ports on the other VLAN-aware network devices along the path that will carry this traffic to the same VLAN(s). However, if you want a port on this switch to participate in one or more VLANs, but none of the intermediate network devices nor the host at the other end of the connection supports VLANs, then you should add this port to the VLAN as an untagged port.

To enable VLANs for this switch, assign each port to the VLAN group(s) in which it will participate.

PARAMETERS

The following parameters are displayed on the Static VLAN page:

- **VLAN ID** - VLAN Identifier. (Range: 1-4095)
- **VLAN Name** - Name of the VLAN (1-100 characters)
- **Port** - Port or trunk identifier. Select VLAN membership for each interface by marking the appropriate radio button for a port or trunk:
  - **Untagged** - Interface is a member of the VLAN. All packets transmitted by the port will be untagged, that is, not carry a tag and therefore not carry VLAN or CoS information. Note that an interface must be assigned to at least one group as an untagged port.
  - **Tagged** - Interface is a member of the VLAN. All packets transmitted by the port will be tagged, that is, carry a tag and therefore carry VLAN or CoS information.
  - **Not Member** - Interface is not a member of the VLAN. Packets associated with this VLAN will not be transmitted by the interface.

NOTE: Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. Note that if you implement VLANs which do not overlap, but still need to communicate, you must connect them through a router.

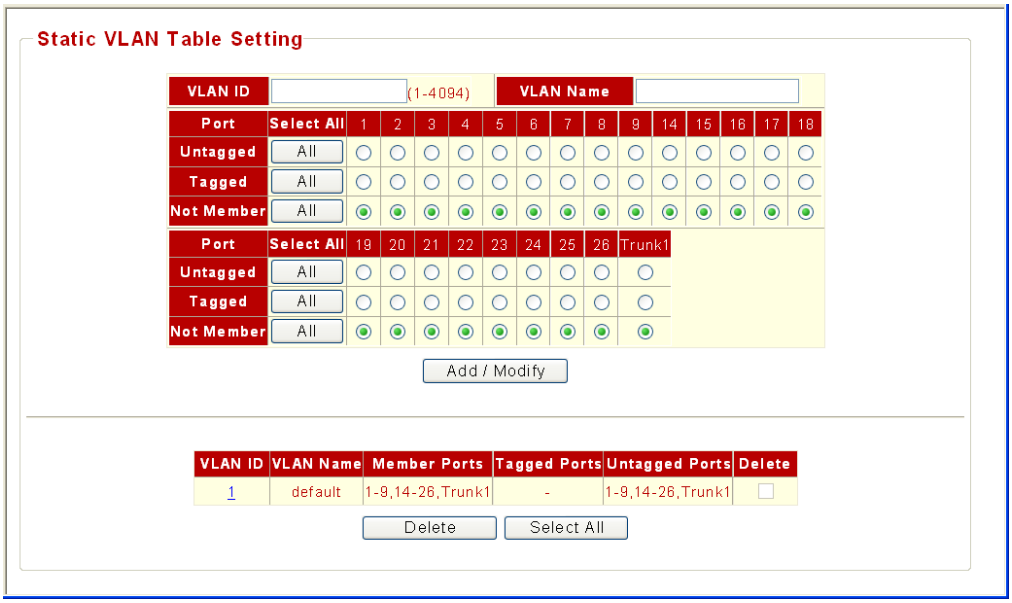
WEB INTERFACE

To configure IEEE 802.1Q VLAN groups:

1. Click Configuration, VLAN, Static VLAN.
2. Select a VLAN ID number.
3. Define a name to identify the VLAN.
4. Mark the ports to be assigned to the new VLAN as tagged or untagged members.
5. Click Add/Modify.

NOTE: To modify a created VLAN, click on the VLAN ID in the current VLAN list to display the current settings.

Figure 15: VLAN Membership Configuration



CONFIGURING VLAN ATTRIBUTES FOR PORT MEMBERS

You can configure VLAN attributes for specific interfaces, including the default Port VLAN identifier (PVID).

PARAMETERS

The following parameters are displayed on the VLAN Setting page:

- **Port** - Selects one or more ports or trunks to configure. Hold down the Ctrl key and click port numbers to selelct multiple ports. Hold down the Shift key to select a range of ports.
- **PVID** - The VLAN ID assigned to untagged frames received on the interface. (Range: 1-4095; Default: 1)

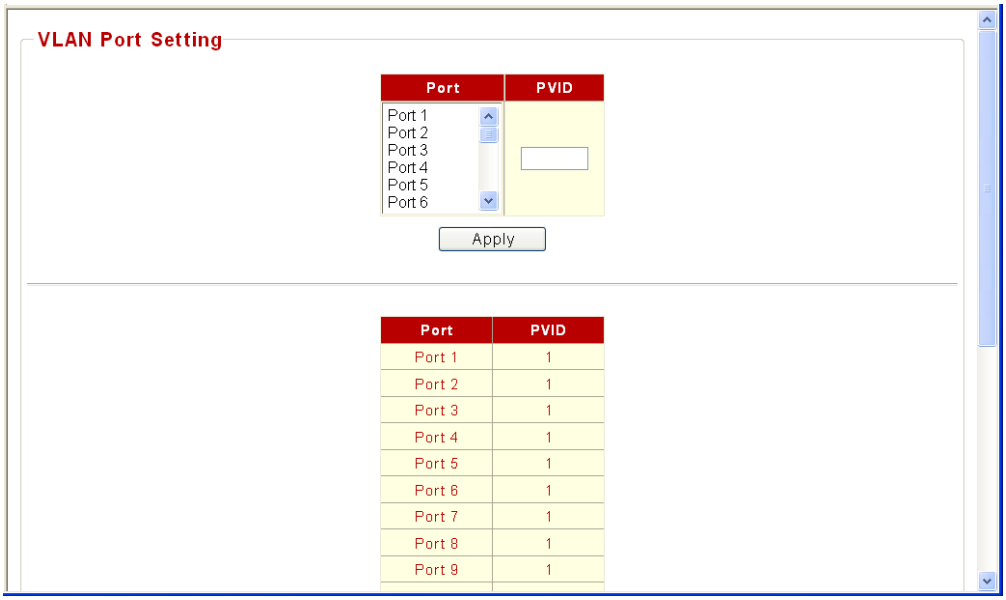
  Ports must be a member of the same VLAN as the Port VLAN ID.

WEB INTERFACE

To configure attributes for VLAN port members:

1. Click Configuration, VLAN, VLAN Setting.
2. Select one or more ports or trunks to configure.
3. Configure the required PVID setting.
4. Click Apply.

Figure 16: VLAN Port Configuration



8 VLAN STACKING

This chapter includes the following sections for configuring VLAN Stacking:

- "Configuring IEEE 802.1Q Tunneling" on page 61
- "VLAN Stacking Table" on page 62
- "VLAN Stacking Settings" on page 63

CONFIGURING IEEE 802.1Q TUNNELING

VLAN Stacking, or IEEE 802.1Q Tunneling (QinQ), is designed for service providers carrying traffic for multiple customers across their networks. QinQ tunneling is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs. This is accomplished by inserting Service Provider VLAN (S-VLAN) tags into the customer's frames when they enter the service provider's network, and then stripping the tags when the frames leave the network.

A service provider's customers may have specific requirements for their internal VLAN IDs and number of VLANs supported. VLAN ranges required by different customers in the same service-provider network might easily overlap, and traffic passing through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations, require intensive processing of VLAN mapping tables, and could easily exceed the maximum VLAN limit of 4096.

QinQ tunneling uses a single Service Provider VLAN (S-VLAN) for customers who have multiple VLANs. Customer VLAN IDs are preserved and traffic from different customers is segregated within the service provider's network even when they use the same customer-specific VLAN IDs. QinQ tunneling expands VLAN space by using a VLAN-in-VLAN hierarchy, preserving the customer's original tagged packets, and adding S-VLAN tags to each frame (also called double tagging).

A port configured to support QinQ tunneling must be set to tunnel port mode. The Service Provider VLAN (S-VLAN) ID for the specific customer must be assigned to the QinQ tunnel access port on the edge switch where the customer traffic enters the service provider's network. Each customer requires a separate S-VLAN, but this VLAN supports all of the customer's internal VLANs. The QinQ tunnel uplink port that passes traffic from the edge switch into the service provider's metro network must also be added to this S-VLAN. The uplink port can be added to multiple S-VLANs to carry inbound traffic for different customers onto the service provider's network.

When a double-tagged packet enters another trunk port in an intermediate or core switch in the service provider's network, the outer tag is stripped for packet processing. When the packet exits another trunk port on the same core switch, the same S-VLAN tag is again added to the packet.

When a packet enters the trunk port on the service provider's egress switch, the outer tag is again stripped for packet processing. However, the S-VLAN tag is not added when it is sent out the tunnel access port on the edge switch into the customer's network. The packet is sent as a normal IEEE 802.1Q-tagged frame, preserving the original VLAN numbers used in the customer's network.

VLAN STACKING TABLE

Sets the stacking VLAN membership for selected interfaces to be part of the Service Provider VLAN (S-VLAN), that is uplink ports for a 802.1Q Tunnel. This stacking VLAN is used to segregate and preserve customer VLAN IDs for traffic crossing the service provider network.

The switch supports up to 64 S-VLAN IDs.

PARAMETERS

The following parameters are displayed on the Static VLAN page:

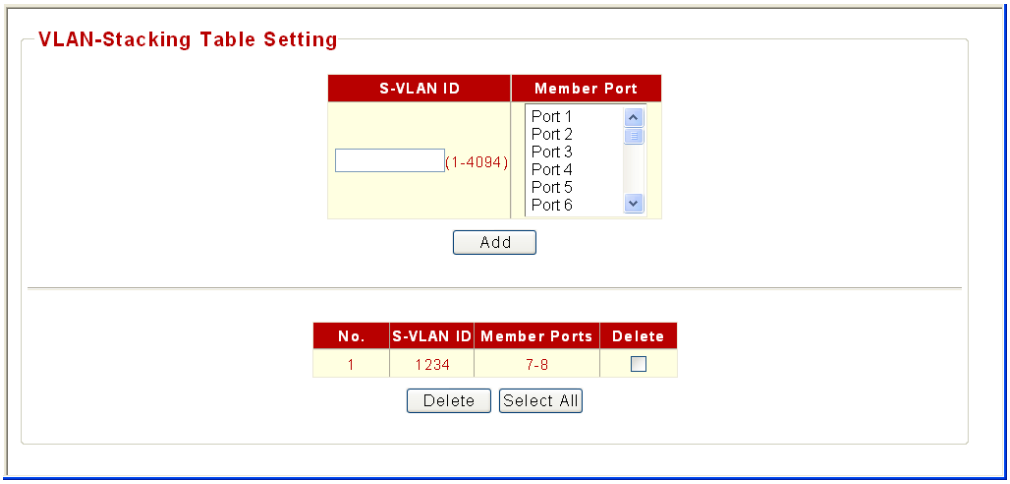
- **S-VLAN ID** - The VLAN identifier of a stacking VLAN. (Range: 1-4094)
- **Member Ports** - Switch ports that are members of the stacking VLAN. That is, ports that will double tag ingress and egress packets.

WEB INTERFACE

To configure stacking VLAN port members:

1. Click Configuration, VLAN Stacking, S-VLAN Table.
2. Specify the S-VLAN ID number.
3. Mark the ports to be included as stacking VLAN port members for specified S-VLAN.
4. Click Add.

Figure 17: VLAN Stacking Table



VLAN STACKING SETTINGS

After configuring port members for stacking VLANs on the switch, the ports connected to a service provider network need to be enabled as doubled-tagged ports. Also the Tag Protocol Identifier (TPID) value must be set for the doubled-tagged ports to identify 802.1Q tagged frames.

PARAMETERS

- **PVID** – The stacking VLAN Port VLAN Identifier. The PVID determines the stacking VLAN tag for single-tagged packets forwarded to an enabled S-VLAN port.

- **Provider Network Port** – Set the S-VLAN membership mode for the selected interface. This mode is used to segregate and preserve customer VLAN IDs for traffic crossing the service provider network. (Default: Disable)

  - **Enable** – Indicates a port linked to a service provider (an 802.1Q Tunnel port).

  - **Disable** – Indicates a port linked to a customer.

- **Tag Protocol ID** – Tag Protocol Identifier specifies the ethertype of incoming packets on a tunnel port. (Range: 0x0600~0xFFFF hexadecimal; Default: 0x88a8)

  Use the TPID field to set a custom 802.1Q ethertype value on the selected interface. This feature allows the switch to interoperate with third-party switches that do not use the standard 0x8100 ethertype to identify 802.1Q-tagged frames. For example, 0x1234 is set as the custom 802.1Q ethertype on a trunk port, incoming frames containing that ethertype are assigned to the VLAN contained in the tag following

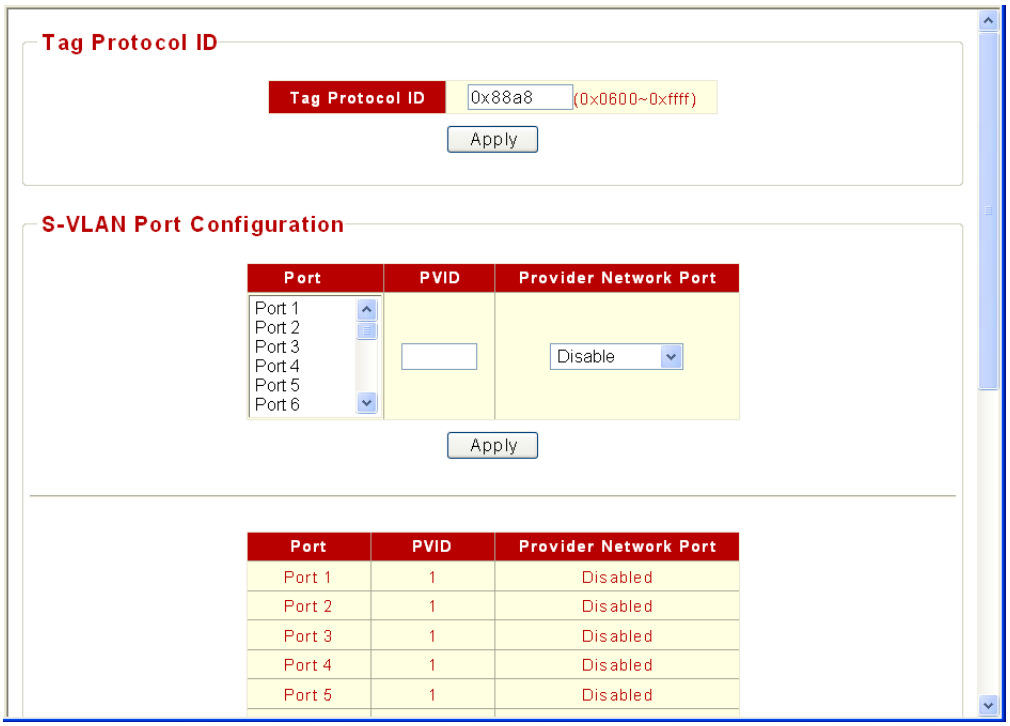
the ethertype field, as they would be with a standard 802.1Q trunk. Frames arriving on the port containing any other ethertype are looked upon as untagged frames, and assigned to the native VLAN of that port.

WEB INTERFACE

To configure stacking VLAN port settings:

1. Click Configuration, VLAN Stacking, S-VLAN Setting.
2. Specify the Tag Protocol ID number.
3. Set the stacking PVID for service provider ports and configure them as "Enabled."
4. Click Apply.

Figure 18: VLAN Stacking Settings



9 IGMP SNOOPING

This chapter includes the following sections for configuring IGMP Snooping:

- "IGMP Snooping Introduction" on page 65
- "Multicast Entry Table" on page 66
- "IGMP Snooping Setting" on page 67

IGMP SNOOPING INTRODUCTION

Multicasting is used to support real-time applications such as videoconferencing or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its service to the network, and any hosts that want to receive the multicast register with their local multicast switch/router. Although this approach reduces the network overhead required by a multicast server, the broadcast traffic must be carefully pruned at every multicast switch/router it passes through to ensure that traffic is only passed on to the hosts which subscribed to this service.

This switch can use Internet Group Management Protocol (IGMP) to filter multicast traffic. IGMP Snooping can be used to passively monitor or "snoop" on exchanges between attached hosts and an IGMP-enabled device, most commonly a multicast router. In this way, the switch can discover the ports that want to join a multicast group, and set its filters accordingly.

If there is no multicast router attached to the local subnet, multicast traffic and query messages may not be received by the switch. In this case (Layer 2) IGMP Query can be used to actively ask the attached hosts if they want to receive a specific multicast service. IGMP Query thereby identifies the ports containing hosts requesting to join the service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service.

The purpose of IP multicast filtering is to optimize a switched network's performance, so multicast packets will only be forwarded to those ports containing multicast group hosts or multicast routers/switches, instead of flooding traffic to all ports in the subnet (VLAN).

MULTICAST ENTRY TABLE

The IGMP Multicast Router Information table displays the current multicast groups learned through IGMP Snooping.

Multicast routers that are attached to ports on the switch use information obtained from IGMP, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet. You can use the IGMP Multicast Router Information table to see which ports on the switch are attached to a neighboring multicast router.

PARAMETERS

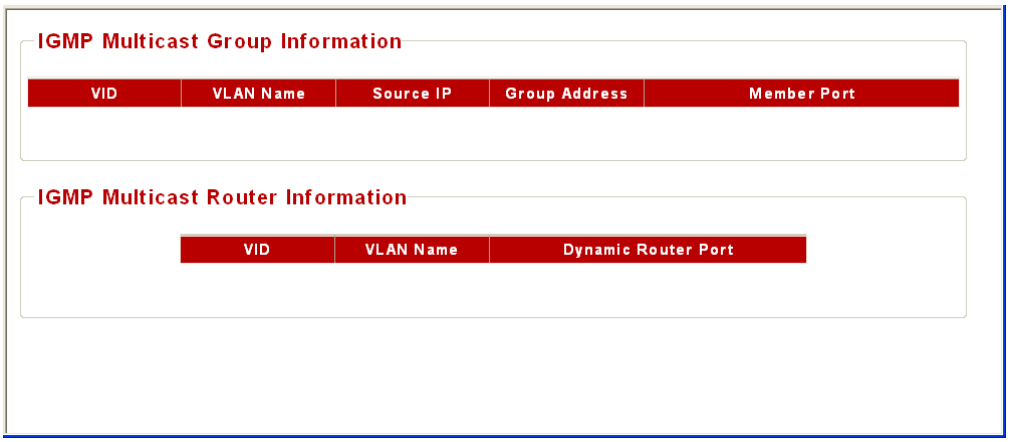
The following parameters are displayed on the Multicast Entry Table page:

- **VID** – A VLAN on the switch that is forwarding multicast traffic to downstream ports for the specified multicast group address.
- **VLAN Name** – The name of the VLAN on the switch that is forwarding multicast traffic.
- **Source IP** – The IP address of one of the multicast servers transmitting traffic to the specified group.
- **Group Address** – IP multicast group address with subscribers directly attached or downstream from the switch, or a static multicast group assigned to this interface.
- **Member Port** – An downstream port that is receiving traffic for the specified multicast group.
- **Dynamic Router Port** – The port interfaces dynamically discovered by the switch to be attached to Multicast routers.

WEB INTERFACE

To display multicast group and router port information, click Configuration, IGMP Snooping, Multicast Entry Table.

Figure 19: Multicast Entry Table



IGMP SNOOPING SETTING

You can configure the switch to forward multicast traffic intelligently. Based on the IGMP query and report messages, the switch forwards traffic only to the ports that request multicast traffic. This prevents the switch from broadcasting the traffic to all ports and possibly disrupting network performance.

If multicast routing is not supported on other switches in your network, you can use IGMP Snooping and IGMP Query to monitor IGMP service requests passing between multicast clients and servers, and dynamically configure the switch ports which need to forward multicast traffic.

Multicast routers use information from IGMP snooping and query reports, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet.

IGMP GLOBAL SETTING

The following parameters are displayed for the Global Setting section of the IGMP Snooping Setting page:

- **IGMP Snooping** - When enabled, the switch will monitor network traffic to determine which hosts want to receive multicast traffic. (Default: Disabled)

  This switch can passively snoop on IGMP Query and Report packets transferred between IP multicast routers/switches and IP multicast host groups to identify the IP multicast group members. The switch monitors the IGMP packets passing through it, picks out the group registration information, and configures the multicast filters accordingly.

- **IGMP Fast-Leave** - Immediately deletes a member port of a multicast service if a leave packet is received on that port. Fast Leave can improve bandwidth usage for a network which frequently experiences many IGMP host add and leave requests. (Default: Disabled)

- **Unknown Multicast** — When the table used to store multicast entries for IGMP snooping is filled, no new entries are learned. If no router port is configured in the attached VLAN, any subsequent multicast traffic not found in the table is either dropped or flooded throughout the VLAN. (Default: Drop)

- **Query Interval** — Sets the frequency at which the switch sends IGMP host-query messages. (Range: 60-600 seconds, Default: 125)

- **Response Time** — Sets the time between receiving an IGMP Report for an IP multicast address on a port before the switch sends an IGMP Query out of that port and removes the entry from its list. (Range: 10-25 seconds, Default: 10)

- **Router Timeout** — The time the switch waits after the previous querier stops before it considers it to have expired. (Range: 60-600 seconds, Default: 125)

- **Last Member Query Interval** — The interval to wait for a response to a group-specific or group-and-source-specific query message. (Range: 1-25 seconds ; Default: 1 second)

- **Robustness Variable** — Specifies the robustness (or expected packet loss) for interfaces. The robustness value is used in calculating the appropriate range for other IGMP variables. (Range: 1-255; Default: 2)

- **Host Timeout** — The time the switch waits for an IGMP report from a host for a multicast group. When IGMP reports are not received, host ports are removed from the member list of that multicast group.

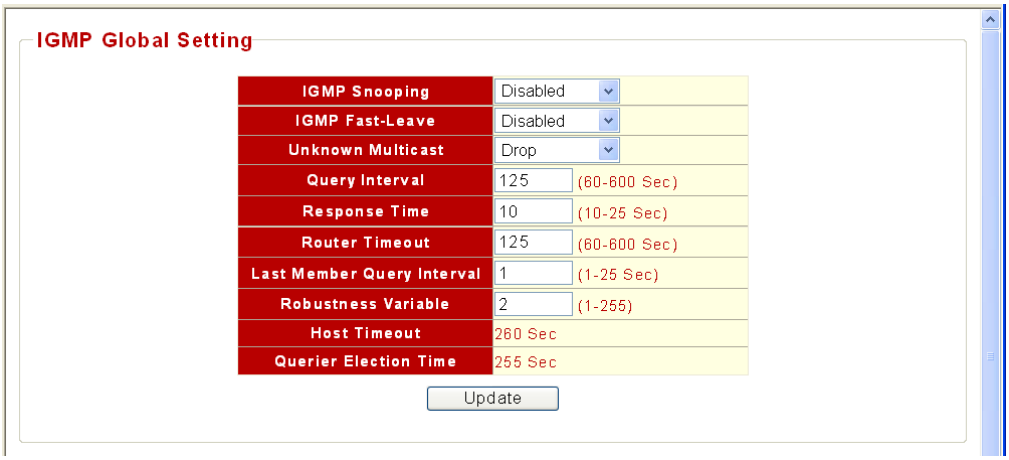
- **Querier Election Time** — The time the switch waits to receive IGMP queries from other routers. If no queries are received, the switch itself will become the querier (when enabled).

WEB INTERFACE

To configure IGMP Snooping global settings:

1. Click Configuration, IGMP Snooping, IGMP Snooping Setting.
2. Enable IGMP Snooping on the switch.
3. Modify other IGMP global settings as required.
4. Click Update.

Figure 20: IGMP Snooping Global Settings



IGMP VLAN SETTING

The following parameters are displayed for the VLAN Setting section of the IGMP Snooping Setting page:

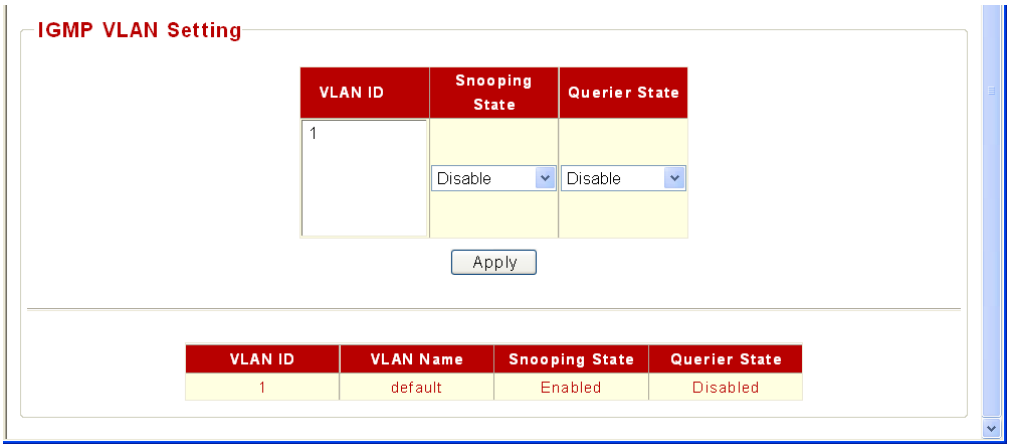
- **VLAN ID** — Specifies the ID of a configured VLAN on the switch. (Range: 1-4094)
- **VLAN Name** — Displays the name of the VLAN.
- **Snooping State** — Enables IGMP snooping on the VLAN. (Default: Disabled)
- **Querier State** — Enables IGMP querier on the VLAN. (Default: Disabled)

WEB INTERFACE

To configure IGMP Snooping settings:

1. Click Configuration, IGMP Snooping, IGMP Snooping Setting.
2. Specify the VLAN ID.
3. Enable IGMP Snooping on the VLAN.
4. Enable IGMP Querier on the VLAN if you want this switch to be elected as querier.
5. Click Apply.

Figure 21: IGMP Snooping VLAN Settings



10 SPANNING TREE

This chapter includes the following sections for configuring Spanning Tree:

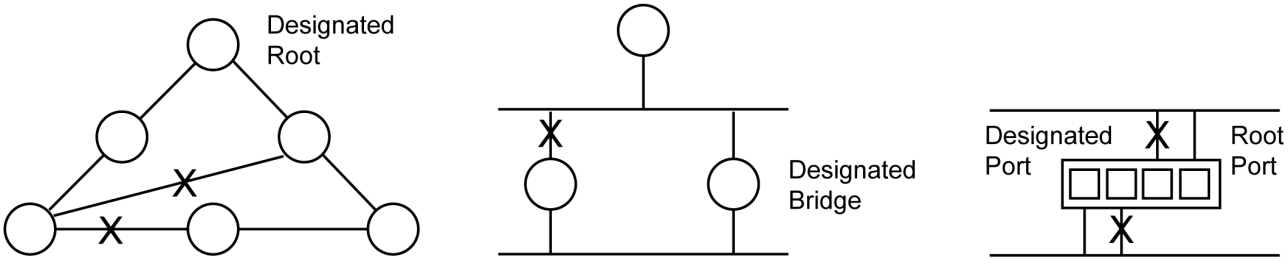
- "Configuring the Spanning Tree Protocol" on page 71
- "Configuring STP Global Settings" on page 72
- "Configuring STP Port Settings" on page 75

CONFIGURING THE SPANNING TREE PROTOCOL

The Spanning Tree Protocol (STP) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices (that is, an STP-compliant switch, bridge or router) in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

This switch supports Rapid Spanning Tree Protocol (RSTP), but is backward compatible with Spanning Tree Protocol (STP).

- **STP** - STP uses a distributed algorithm to select a bridging device (STP-compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.



Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

- **RSTP** - RSTP is designed as a general replacement for the slower, legacy STP. RSTP is also incorporated into MSTP (Multiple Spanning Tree Protocol). RSTP achieves must faster reconfiguration (i.e., around 1 to 3 seconds, compared to 30 seconds or more for STP) by reducing the number of state changes before active ports start learning, predefining an alternate route that can be used when a node or port fails, and retaining the forwarding database for ports insensitive to changes in the tree structure when reconfiguration occurs.

CONFIGURING STP GLOBAL SETTINGS

Use the STP Global Setting page to configure settings for STP which apply globally to the switch.

PARAMETERS

The following parameters are displayed on the STP Global Setting page:

- **Spanning Tree Status** — Enables Spanning Tree on the switch. (Default: Disabled)
- **Force Version** — Specifies the type of spanning tree used on this switch. RSTP supports connections to either RSTP or STP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below. (Options: RSTP or STP; Default: RSTP)
  - **RSTP Mode** — If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.
  - **STP Mode** — If the switch receives an 802.1D BPDU (i.e., STP BPDU) after a port's migration delay timer expires, the switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.
- **Priority** — Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STP root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. Note that lower numeric values indicate higher priority.
(Options: 0-61440, in steps of 4096; Default: 32768)

- **Maximum Age** — The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STP information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. (Note that references to "ports" in this section mean "interfaces," which includes both ports and trunks.)

  Minimum: The higher of 6 or [2 x (Hello Time + 1)]
  Maximum: The lower of 40 or [2 x (Forward Delay - 1)]
  Default: 20

- **Hello Time** — The interval (in seconds) at which the root device transmits a configuration message.

  Default: 2
  Minimum: 1
  Maximum: The lower of 10 or [(Max. Message Age / 2) -1]

- **Forward Delay** — The maximum time (in seconds) this device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.

  Minimum: The higher of 4 or [(Max. Message Age / 2) + 1]
  Maximum: 30
  Default: 15

- **Root Priority** — The priority of the device in the Spanning Tree that this switch has accepted as the root device.

- **Root MAC Address** — The MAC address of the device in the Spanning Tree that this switch has accepted as the root device.

- **Root Path Cost** — The path cost from the root port on this switch to the root device.

- **Root Port** — The number of the port on this switch that is closest to the root. This switch communicates with the root device through this port. If there is no root port, then this switch has been accepted as the root device of the Spanning Tree network.

- **Root Maximum Age** — The maximum time (in seconds) this device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. If the root port ages out STA information (provided in the last configuration message), a new root port is selected from among the device ports attached to the

network. (References to "ports" in this section means "interfaces," which includes both ports and trunks.)

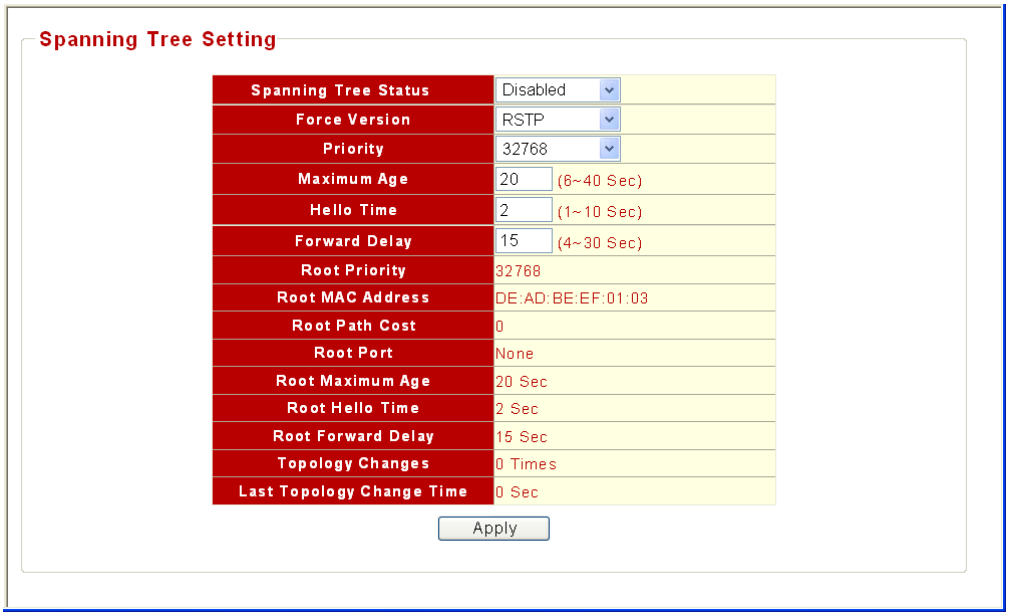
- **Root Hello Time** — The interval (in seconds) at which this device transmits a configuration message.
- **Root Forward Delay** — The maximum time (in seconds) this device will wait before changing states (i.e., discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.
- **Topology Changes** — The number of times the Spanning Tree has been reconfigured.
- **Last Topology Change Time** — The time since the Spanning Tree was last reconfigured.

WEB INTERFACE

To configure global settings for Spanning Tree:

1. Click Configuration, Spanning Tree, STP Global Setting.
2. Set the Spanning Tree Status to enabled.
3. Modify other required parameters.
4. Click Apply.

Figure 22: STP Global Setting



CONFIGURING STP PORT SETTINGS

Use the STP Port Setting page to configure Spanning Tree attributes for specific interfaces, including path cost, port priority, edge port (for fast forwarding), automatic detection of an edge port, and point-to-point link type.

PARAMETERS

The following parameters are displayed on the STP Port Setting page:

- **Port** — Port identifier. (Range: 1-26)

  This field is not applicable to static trunks or dynamic trunks created through LACP. Also, note that only one set of interface configuration settings can be applied to all trunks.

- **Path Cost** — This parameter is used by the STP to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.)

  By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below.

Table 5: Recommended STP Path Cost Range

Port Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	50-600	200,000-20,000,000
Fast Ethernet	10-60	20,000-2,000,000
Gigabit Ethernet	3-10	2,000-200,000

Table 6: Recommended STP Path Costs

Port Type	Link Type	IEEE 802.1D-1998	IEEE 802.1w-2001
Ethernet	Half Duplex	100	2,000,000
	Full Duplex	95	1,999,999
	Trunk	90	1,000,000
Fast Ethernet	Half Duplex	19	200,000
	Full Duplex	18	100,000
	Trunk	15	50,000
Gigabit Ethernet	Full Duplex	4	10,000
	Trunk	3	5,000

Table 7: Default STP Path Costs

Port Type	Link Type	IEEE 802.1w-2001
Ethernet	Half Duplex Full Duplex Trunk	2,000,000 1,000,000 500,000
Fast Ethernet	Half Duplex Full Duplex Trunk	200,000 100,000 50,000
Gigabit Ethernet	Full Duplex Trunk	10,000 5,000

- **Priority** — Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on a switch are the same, the port with the highest priority (i.e., lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled. (Range: 0-240, in steps of 16; Default: 128)

- **P2P** — The link type attached to an interface can be set to automatically detect the link type, or manually configured as point-to-point or shared medium. Transition to the forwarding state is faster for point-to-point links than for shared media. These options are described below:

  - **Auto** — The switch automatically determines if the interface is attached to a point-to-point link or to shared medium. (This is the default setting.)

  - **True** — A point-to-point connection to exactly one other bridge.

  - **False** — A shared connection to two or more bridges.

- **Edge** (Fast Forwarding) — You can enable this option if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying edge ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STP-related timeout problems. However, remember that this feature should only be enabled for ports connected to an end-node device. (Default: False)

- **State** — Displays current state of this port within the Spanning Tree:

  - **Disabled** — There is no connection on the port.

- **Discarding** — Port receives STP configuration messages, but does not forward packets.
- **Learning** — Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
- **Forwarding** — Port forwards packets, and continues learning addresses.

The rules defining port status are:

- A port on a network segment with no other STP compliant bridging device is always forwarding.
- If two ports of a switch are connected to the same segment and there is no other STP device attached to this segment, the port with the smaller ID forwards packets and the other is discarding.
- All ports are discarding when the switch is booted, then some of them change state to learning, and then to forwarding.

- **Role** — Roles are assigned according to whether the port is part of the active topology connecting the bridge to the root bridge (that is, **root** port), connecting a LAN through the bridge to the root bridge (that is, **designated** port), or is an **alternate** or **backup** port that may provide connectivity if other bridges, bridge ports, or LANs fail or are removed. The role is set to disabled (that is, **disabled** port) if a port has no role within the spanning tree.
- **Path Cost** — The path cost setting for the port:
  - **Config** — The administrator configured path cost setting.
  - **Actual** — The contribution of this port to the path cost of paths towards the spanning tree root which include this port.
- **Priority** — Defines the priority used for this port in the Spanning Tree. If the path cost for all ports on a switch is the same, the port with the highest priority (that is, lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with the lowest numeric identifier will be enabled.
- **P2P** — The point-to-point setting for the port:
  - **Config** — The administrator configured P2P setting.
  - **Actual** – The operational point-to-point status of the LAN segment attached to this interface. This parameter is determined by manual configuration or by auto-detection.

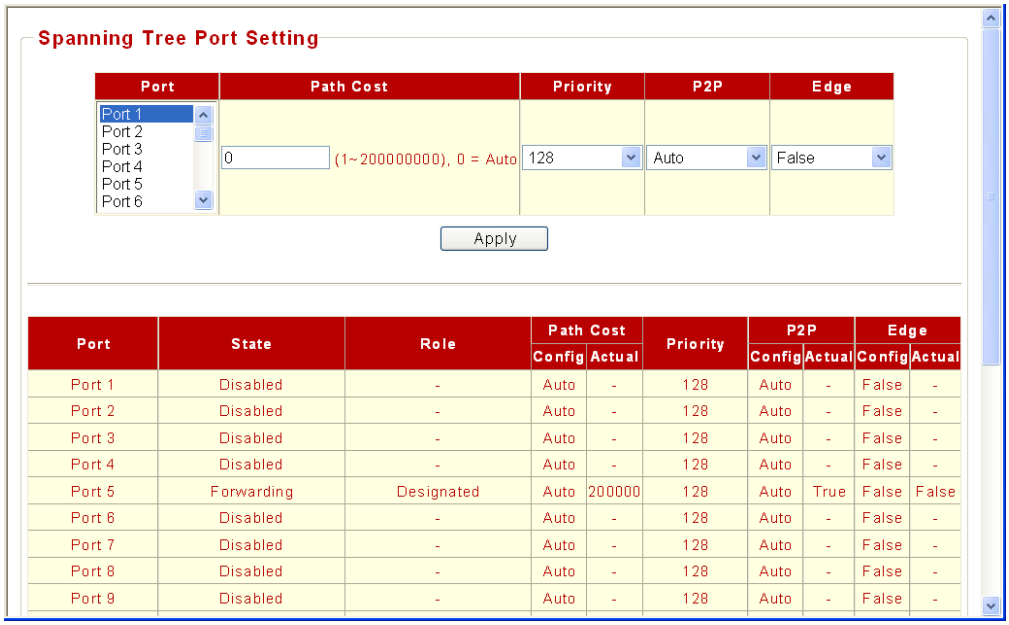
- **Edge** — The Edge setting for the port:
  - **Config** — The administrator configured Edge setting.
  - **Actual** — This parameter is initialized to the port setting for Edge (that is, True or False), but will be set to false if a BPDU is received, indicating that another bridge is attached to this port.

WEB INTERFACE

To configure port settings for Spanning Tree:

1. Click Configuration, Spanning Tree, STP Port Setting.
2. Modify the required attributes for one or a group of ports.
3. Click Apply.

Figure 23: STP Port Setting



11 QUALITY OF SERVICE

This chapter includes the following sections for configuring Quality of Service (QoS):

- "QoS Introduction" on page 79
- "Port-Based Priority" on page 80
- "DSCP-Based Priority" on page 81
- "Priority-to-Queue Mapping" on page 82
- "Packet Scheduling" on page 84

QOS INTRODUCTION

All switches or routers that access the Internet rely on class information to provide the same forwarding treatment to packets in the same class. Class information can be assigned by end hosts, or switches or routers along the path. Priority can then be assigned based on a general policy, or a detailed examination of the packet. However, note that detailed examination of packets should take place close to the network edge so that core switches and routers are not overloaded.

Switches and routers along the path can use class information to prioritize the resources allocated to different traffic classes. The manner in which an individual device handles traffic is called per-hop behavior. All devices along a path should be configured in a consistent manner to construct a consistent end-to-end Quality of Service (QoS) solution.

This section describes how to specify which data packets have greater precedence when traffic is buffered in the switch due to congestion. This switch provides eight priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. You can set the default priority for each interface, the queuing mode, and queue weights.

PORT-BASED PRIORITY

You can specify the default port priority for each port on the switch, a Quality Control List (which sets the priority for ingress packets based on detailed criteria), the default tag assigned to egress packets, the queuing mode, and queue weights.

PARAMETERS

The following parameters are displayed on the Port-Based Priority page:

- **Port** — Port identifier.
- **Priority** — The default priority used when adding a tag to untagged frames. (Range: 0-7; Default: 0)

  The default tag priority applies to untagged frames received on a port set to accept all frame types (that is, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.

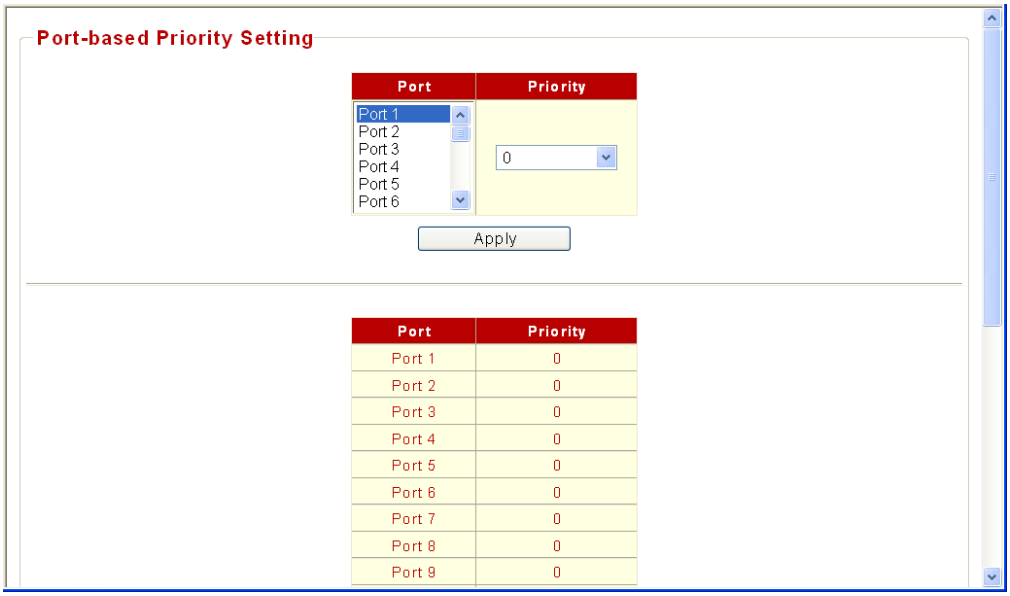
  Inbound frames that do not have VLAN tags are tagged with the input port's default ingress tag priority, and then placed in the appropriate priority queue at the output port. (Note that if the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.)

WEB INTERFACE

To configure global settings for Spanning Tree:

1. Click Configuration, QoS, Port-based Priority.
2. For one or a group of ports, set the default priority value.
3. Click Apply.

Figure 24: Port-Based Priority Setting



DSCP-BASED PRIORITY

The Differentiated Services Code Point (DSCP) is a six-bit field in the IP header, allowing coding for up to 64 different forwarding behaviors. The DSCP replaces the ToS bits, but it retains backward compatibility with the three precedence bits so that non-DSCP compliant, ToS-enabled devices, will not conflict with the DSCP mapping. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. Note that all the DSCP values that are not specified are mapped to priority value 0.

PARAMETERS

The following parameters are displayed on the DSCP-Based Priority page:

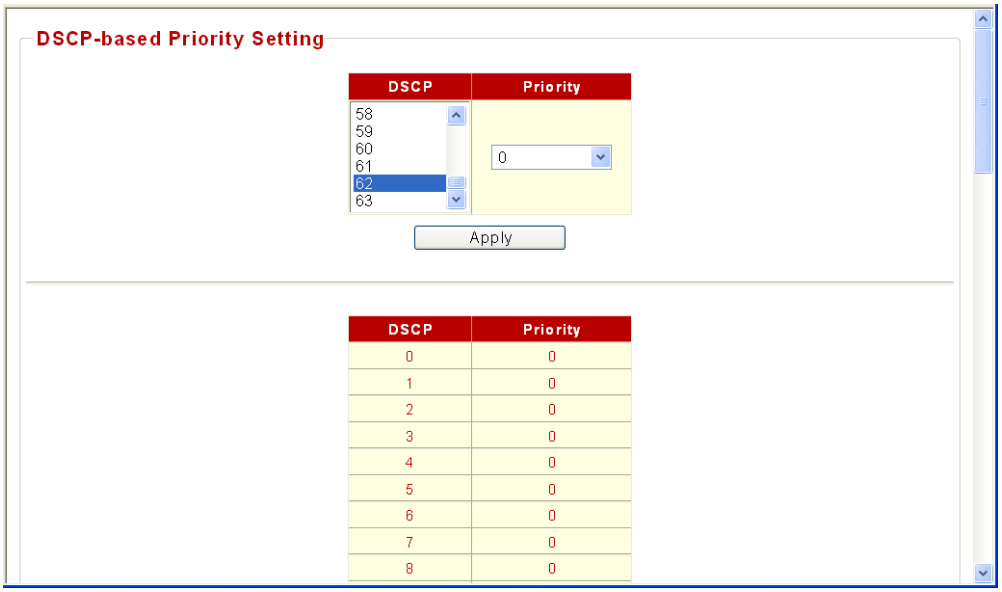
- **DSCP —** Lists the DSCP values. (Range: 0-63)
- **Priority —** Maps a priority value to the selected DSCP Priority value. Note that "0" represents low priority and "7" represent high priority.
- **DSCP Priority Table —** Shows the DSCP to Priority map.

WEB INTERFACE

To configure port-level DSCP remarking:

1. Click Configuration, QoS, DSCP-based Priority.
2. Map one or more DSCP values to a priority value.
3. Click Apply.

Figure 25: DSCP-Based Priority Setting



PRIORITY-TO-QUEUE MAPPING

This switch processes Class of Service (CoS) priority tagged traffic by using eight priority queues for each port, with service schedules based on Weighted Fair Queuing (WFQ) or Weighted Round Robin (WRR). Up to eight separate traffic priorities are defined in IEEE 802.1p. The default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown in the following table.

Table 8: Default Mapping of CoS Values to Egress Queues

Priority	0	1	2	3	4	5	6	7
Queue	1	2	3	4	5	6	7	8

The priority levels recommended in the IEEE 802.1p standard for various network applications are shown in the following table. However, you can map the priority levels to the switch's output queues in any way that benefits application traffic for your own network.

Table 9: CoS Priority Levels

Priority Level	Traffic Type
1	Background
2	(Spare)
0 (default)	Best Effort
3	Excellent Effort
4	Controlled Load
5	Video, less than 100 milliseconds latency and jitter
6	Voice, less than 10 milliseconds latency and jitter
7	Network Control

PARAMETERS

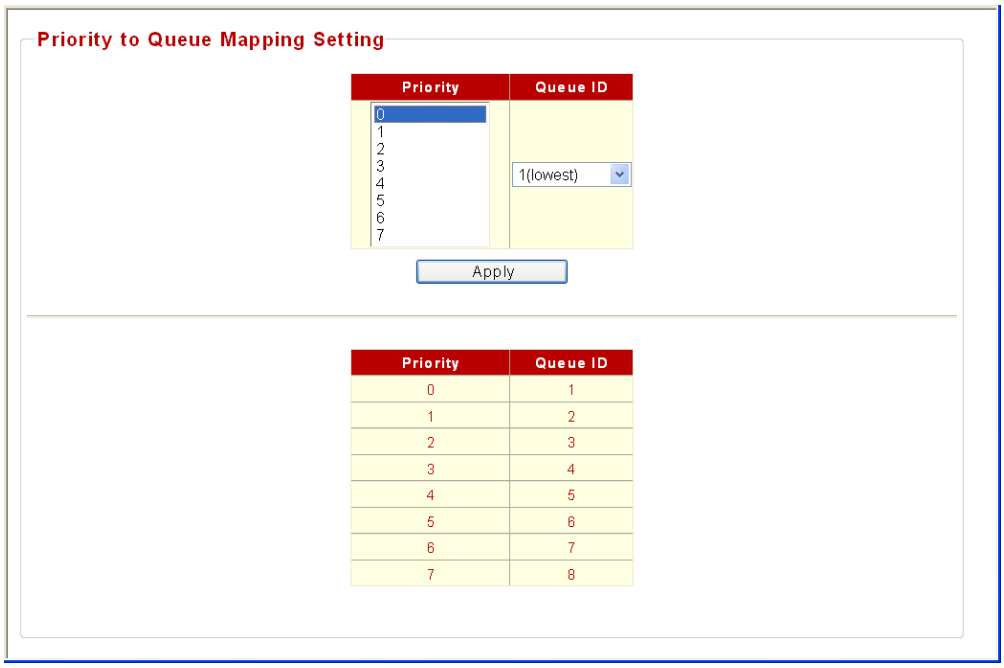
- **Priority** — CoS value. (Range: 0-7, where 7 is the highest priority)
- **Queue ID** — Output queue buffer. (Range: 1-8, where 8 is the highest priority queue)

WEB INTERFACE

To configure port-level DSCP remarking:

1. Click Configuration, QoS, Priority to Queue Mapping.
2. Map one or more priority values to a queue ID.
3. Click Apply.

Figure 26: Priority-to-Queue Mapping



PACKET SCHEDULING

You can set the switch to service the queues based on a strict rule that requires all traffic in a higher priority queue to be processed before lower priority queues are serviced, Weighted Fair Queuing (WFQ), or Weighted Round-Robin (WRR) queuing that specifies a relative weight of each queue.

The traffic classes are mapped to one of the eight egress queues provided for each port. You can assign a weight to each of these queues (and thereby to the corresponding traffic priorities). This weight sets the frequency at which each queue will be polled for service, and subsequently affects the response time for software applications assigned a specific priority value.

PARAMETERS

- **Scheduling Algorithm** — Selects the service method used for port egress queues.
  - **Weight-fair-queue** — Services the egress queues containing data based on the weight of the queue compared to the sum of the weights of all queues. (This is the default selection.)
  - **Weight-round-robin** — Shares bandwidth at the egress ports by using the scheduling weights for queues 1 through 8 respectively. WRR specifies a relative weight for each queue that determines the

percentage of service time the switch services each queue before moving on to the next queue.

- **Queue ID** — Output queue buffer. (Range: 1-8, where 8 is the highest priority queue)
- **Weight** — Set a new weight for the selected traffic class. (Range: Strict or 1-15)

  Use queue weights 1-15 for queues to allocate service time based on WFQ or WRR. Queue weights must be configured in ascendant manner, assigning more weight to each higher numbered queue.

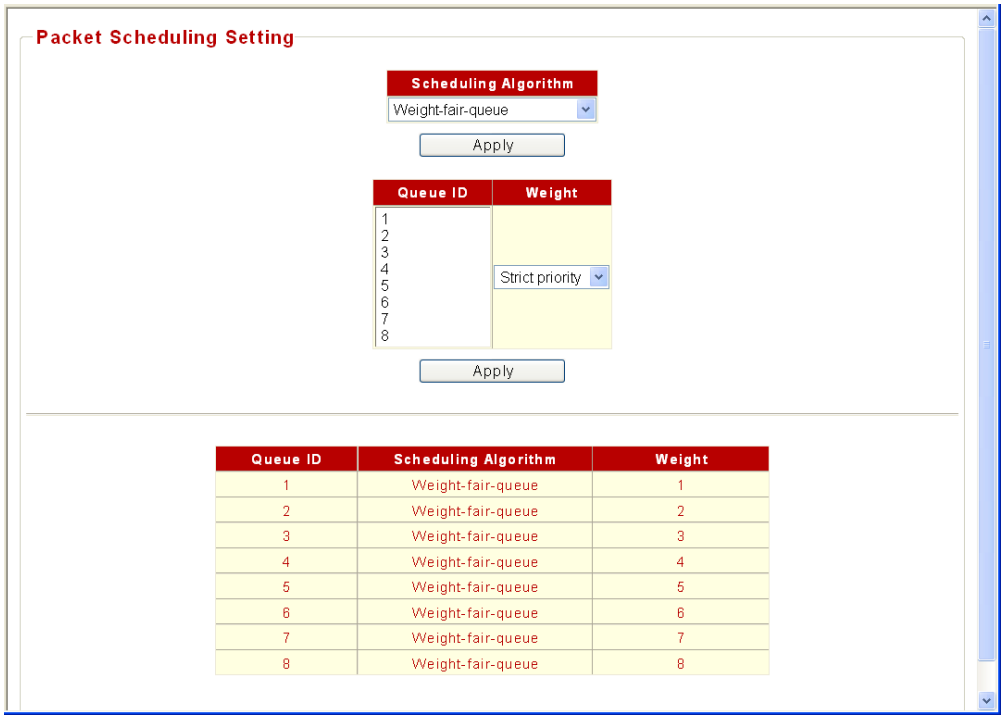
  Strict priority requires all traffic in the queue to be processed before lower priority queues are serviced.

WEB INTERFACE

To configure port-level DSCP remarking:

1. Click Configuration, QoS, Packet Scheduling.
2. Select the scheduling algorithm, WFQ or WRR.
3. Map scheduling weights to a queue ID, or select "Strict."
4. Click Apply.

Figure 27: Packet Scheduling



12 LINK LAYER DISCOVERY PROTOCOL

This chapter includes the following sections for configuring Link Layer Discovery Protocol (LLDP):

- "Configuring LLDP" on page 87
- "LLDP Neighbors" on page 89

CONFIGURING LLDP

The Link Layer Discovery Protocol (LLDP) is used to discover basic information about neighboring devices on the local broadcast domain. LLDP is a Layer 2 protocol that uses periodic broadcasts to advertise information about the sending device. Advertised information is represented in Type Length Value (TLV) format according to the IEEE 802.1AB standard, and can include details such as device identification, capabilities and configuration settings. LLDP also defines how to store and maintain information gathered about the neighboring network nodes it discovers.

PARAMETERS

The following parameters are displayed on the LLDP Configuration page:

- **LLDP Status** — Enables LLDP on the switch. (Default: Disabled)
- **Transmission Interval** — Configures the periodic transmit interval for LLDP advertisements. (Range: 5-32768 seconds; Default: 30 seconds)

  This attribute must comply with the following rule:

  (Transmission Interval * Transmission Hold Time) ≤ 65536,
  and Transmission Interval ≥ (4 * Transmission Delay)
- **Hold Time Multiplier** — Configures the time-to-live (TTL) value sent in LLDP advertisements as shown in the formula below. (Range: 2-10; Default: 3)

  The time-to-live tells the receiving LLDP agent how long to retain all information pertaining to the sending LLDP agent if it does not transmit updates in a timely manner.

  TTL in seconds is based on the following rule:

  (Transmission Interval * Transmission Hold Time) ≤ 65536.
  Therefore, the default TTL is 30*3 = 90 seconds.

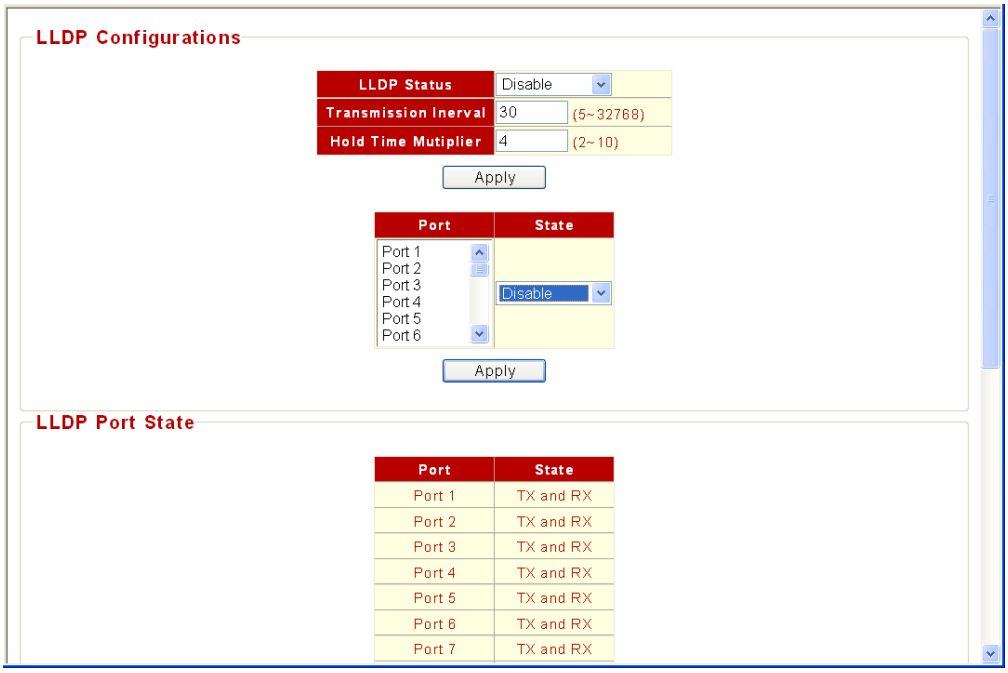
- **Port** — Port identifier. (Range: 1-26)
- **State** — Enables LLDP message transmit and receive modes for LLDP Protocol Data Units. (Options: Disabled, Tx/Rx, Rx only, Tx only; Default: Disabled)

WEB INTERFACE

To configure global and port settings for LLDP:

1. Click Configuration, LLDP, LLDP Settings.
2. Enable LLDP for the switch.
3. If required, modified other LLDP parameters.
4. For one or a group of ports, set the LLDP mode.
5. Click Apply.

Figure 28: LLDP Settings



LLDP NEIGHBORS

Use the LLDP Neighbors page to display information about devices connected directly to the switch's ports which are advertising information through LLDP.

PARAMETERS

The following parameters are displayed on the LLDP Neighbors page:

- **Local Port** — The local port to which a remote LLDP-capable device is attached.
- **Chassis ID** — An octet string indicating the specific identifier for the particular chassis in this system.
- **Remote Port ID** — A string that contains the specific identifier for the port from which this LLDPDU was transmitted.
- **Port Description** — A string that indicates the port's description. If RFC 2863 is implemented, the ifDescr object should be used for this field.
- **System Name** — An string that indicates the system's configures assigned name.
- **System Capabilities** — The capabilities that define the primary function(s) of the system. Refer to the following table:

Table 10: LLDP System Capabilities

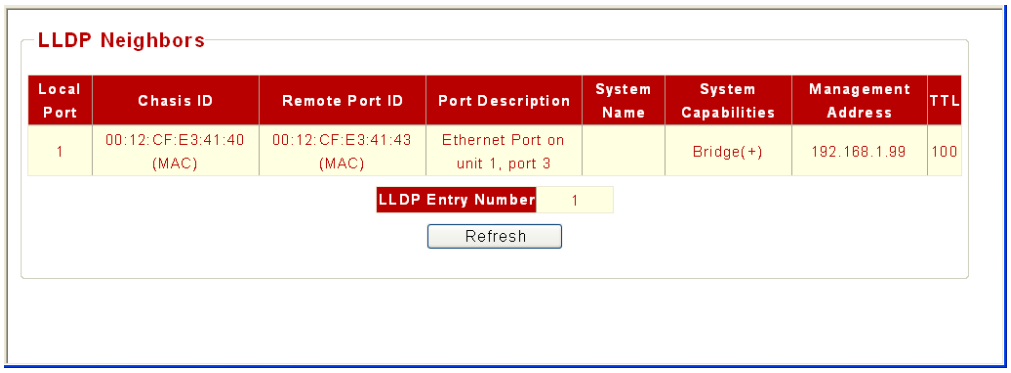
ID Basis	Reference
Other	—
Repeater	IETF RFC 2108
Bridge	IETF RFC 2674
WLAN Access Point	IEEE 802.11 MIB
Router	IETF RFC 1812
Telephone	IETF RFC 2011
DOCSIS cable device	IETF RFC 2669 and IETF RFC 2670
End Station Only	IETF RFC 2011

- **Management Address** — The IPv4 address of the remote device. If no management address is available, the address should be the MAC address for the CPU or for the port sending this advertisement.
- **TTL** — Indicates the time (in seconds) the remote device's information should be treated as valid.
- **LLDP Entry Number** — The number of the LLDP table entry.

WEB INTERFACE

To display LLDP neighbors, click Configuration, LLDP, LLDP Neighbors. Use the Refresh button to update the LLDP information.

Figure 29: LLDP Neighbors



13 SNMP SETTINGS

This chapter includes the following sections for configuring Simple Network Management Protocol (SNMP):

- "Simple Network Management Protocol" on page 91
- "Setting SNMP System and Community Strings" on page 92
- "Specifying SNMP Trap Receivers" on page 93

SIMPLE NETWORK MANAGEMENT PROTOCOL

Simple Network Management Protocol (SNMP) is a communication protocol designed specifically for managing devices on a network. Equipment commonly managed with SNMP includes switches, routers and host computers. SNMP is typically used to configure these devices for proper operation in a network environment, as well as to monitor them to evaluate performance or detect potential problems.

Managed devices supporting SNMP contain software, which runs locally on the device and is referred to as an agent. A defined set of variables, known as managed objects, is maintained by the SNMP agent and used to manage the device. These objects are defined in a Management Information Base (MIB) that provides a standard presentation of the information controlled by the agent. SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network.

The switch includes an onboard agent that supports SNMP versions 1 and 2c. This agent continuously monitors the status of the switch hardware, as well as the traffic passing through its ports. A network management station can access this information using software such as HP OpenView. Access to the onboard agent from clients using SNMP v1 and v2c is controlled by community strings. To communicate with the switch, the management station must first submit a valid community string for authentication.

SETTING SNMP SYSTEM AND COMMUNITY STRINGS

To manage the switch through SNMP, you must first enable the protocol and configure the basic access parameters.

You can configure community strings authorized for management access by clients using SNMP v1 and v2c. All community strings used for IP Trap Receivers should be listed in this table. For security reasons, you should consider removing the default strings.

PARAMETERS

The following parameters are displayed on the SNMP Setting page:

- **SNMP Status** - Enables or disables SNMP service. (Default: Disabled)
- **System Name** – A name assigned to the switch system.
- **System Location** – Specifies the system location.
- **System Contact** – An administrator responsible for the system.
- **String** – A community string that acts like a password and permits access to the SNMP protocol.

  Default strings: "public" (read-only access), "private" (read-write access)

  Range: 1-32 characters, case sensitive

- **Type** – Specifies the access rights for the community string:
  - **Read-Only** – Authorized management stations are only able to retrieve MIB objects.
  - **Read-Write** – Authorized management stations are able to both retrieve and modify MIB objects.

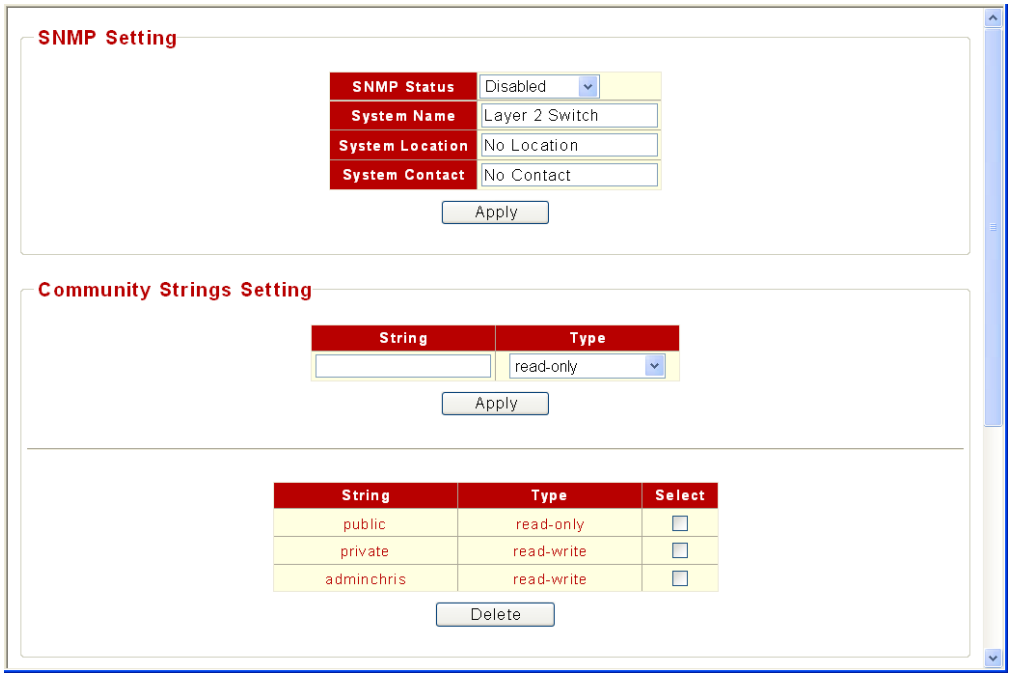
WEB INTERFACE

To configure SNMP system settings:

1. Click Configuration, SNMP Setting.
2. Enable SNMP for the switch.
3. Configure the Name, Location, and Contact information.
4. Define at least one new community string with read-write access.
5. Delete the default "private" string for security reasons.

6. Click Apply.

Figure 30: SNMP Settings



SPECIFYING SNMP TRAP RECEIVERS

Traps indicating status changes are issued by the switch to specified trap managers. You must specify trap managers so that key events are reported by this switch to your management station (using network management software).

PARAMETERS

The following parameters are displayed on the SNMP Setting page for trap receiver configuration:

- **IP Address** – IP address of a new management station to receive notification messages.
- **Community String** – Specifies a valid community string for the new trap manager entry. The string must already be defined in the Community String Setting section. (Range: 1-32 characters, case sensitive)

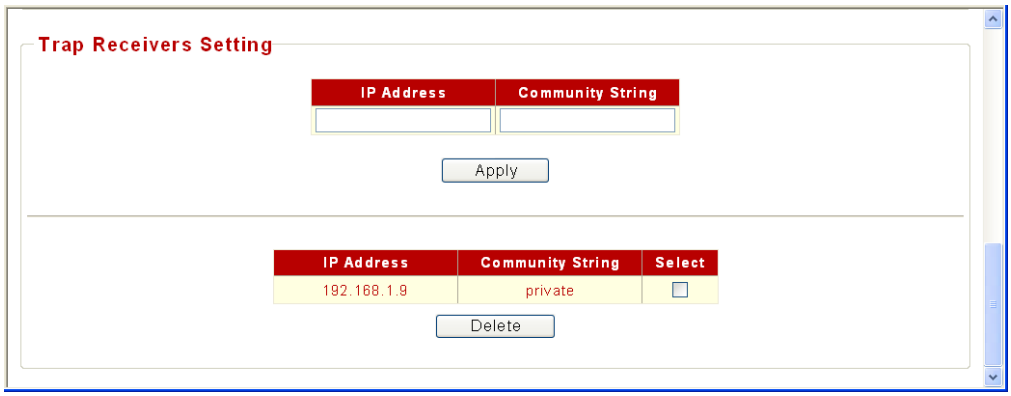
WEB INTERFACE

To configure SNMP system settings:

1. Click Configuration, SNMP Setting.

2. Specify the IP address of management station that will receive SNMP trap messages.
3. Specify a configured community string for the trap receiver.
4. Click Apply.

Figure 31: SNMP Trap Receiver Settings



14 PORT MIRRORING

You can mirror traffic from one or more source ports to a target port for real-time analysis. You can then attach a logic analyzer or RMON probe to the target port and study the traffic crossing the source ports in a completely unobtrusive manner.

USAGE GUIDELINES

- The destination port speed should match or exceed source port speed, otherwise traffic may be dropped from the monitor port.
- Two mirror sessions can be configured.
- All mirrored ports share the same destination port.

PARAMETERS

The following parameters are displayed on the Port Mirroring page:

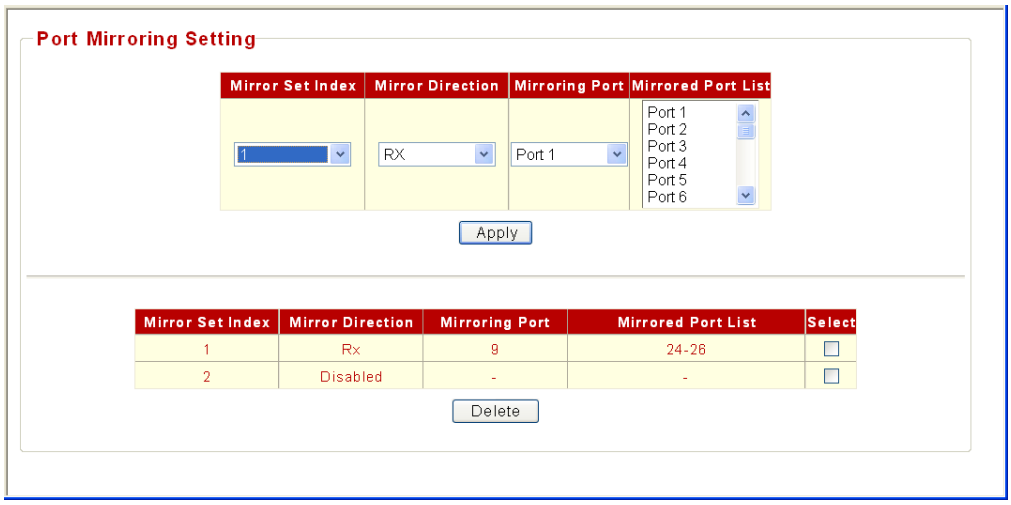
- **Mirror Set Index** — Displays a list of current mirror sessions.
- **Mirror Direction** — Allows you to select which traffic to mirror to the target port, Rx (receive) or Tx (transmit). (Default: Rx)
- **Mirrored Port List** — One or more source ports whose traffic will be monitored. (Range: 1-26 and configured trunks)
- **Mirroring Port** — The target port that will mirror the traffic on the source ports. (Range: 1-26)

WEB INTERFACE

To configure port mirroring:

1. Click Configuration, Port Mirroring.
2. Select the Mirror Set Index.
3. Select the Mirror Direction.
4. Select the Mirroring (target) port.
5. Select the one or more mirrored (source) ports.
6. Click Apply.

Figure 32: Port Mirroring



15 PORT SECURITY

Port security is a feature that allows you to configure a switch port with a maximum number of device MAC addresses that are authorized to access the network through that port.

When port security is enabled on a port, the switch stops learning new MAC addresses on the specified port when it has reached a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table will be accepted as authorized to access the network through that port. If a device with an unauthorized MAC address attempts to use the switch port, the intrusion will be detected and the switch can automatically take a specified action.

To use port security, specify a maximum number of addresses to allow on the port and then let the switch dynamically learn the <source MAC address, VLAN> pair for frames received on the port. Note that you can also manually add secure addresses to the port using the Static Address Table (see "Static MAC Addresses" on page 106). When the port has reached the maximum number of MAC addresses the selected port will stop learning. The MAC addresses already in the address table will be retained and will not age out. Any other device that attempts to use the port will be prevented from accessing the switch.

PARAMETERS

The following parameters are displayed on the Port Security page:

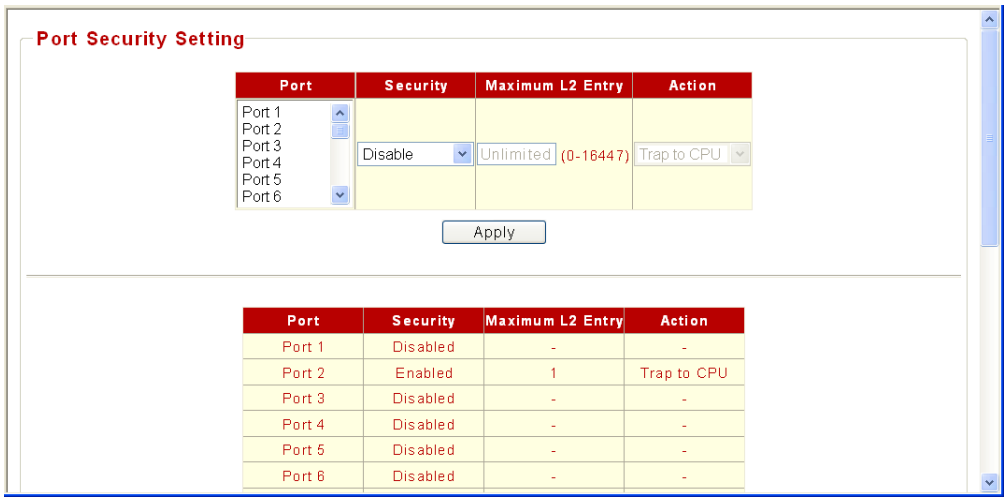
- **Port** — Port number.
- **Security** — Enables or disables port security for the selected ports. (Default: Disabled)
- **Maximum L2 Entry** — The maximum number of MAC addresses that can be learned on a port. (Range: 0 - 16447, where 0 means disabled)
- **Action** — Indicates the action to be taken when a port security violation is detected:
  - **Trap to CPU**: Send an SNMP trap message. (This is the default.)
  - **Drop**: Drop other traffic from the port.
  - **Forward**: No action is taken. Traffic is forwarded as normal.

WEB INTERFACE

To configure port security:

1. Click Configuration, Port Security.
2. Select the ports to configure.
3. Set Security to Enable.
4. Configure the maximum number of MAC addresses allowed on the port.
5. Set an action for port security violations.
6. Click Apply.

Figure 33: Port Security



16 BANDWIDTH CONTROL

This function allows the network manager to control the maximum rate for traffic received on a port or transmitted from a port. Rate limiting is configured on ports at the edge of a network to limit traffic into or out of the switch. Packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports or trunks. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped, conforming traffic is forwarded without any changes.

Input and output rate limits can be enabled or disabled for individual interfaces.

PARAMETERS

The following parameters are displayed on the Bandwidth Control page:

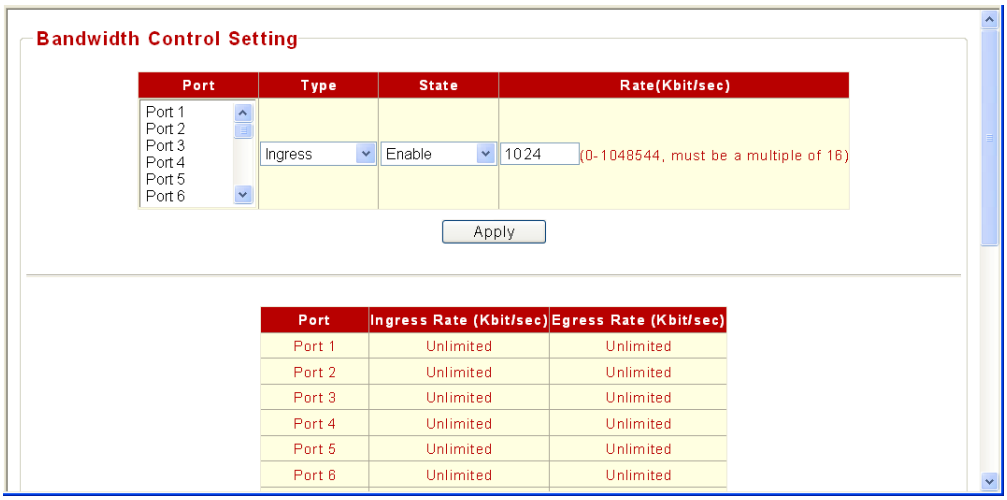
- **Port** — Displays the port/trunk number.
- **Type** — Specifies ingress or egress traffic. (Default: Ingress)
- **State** – Enables or disables the rate limit. (Default: Disabled)
- **Rate (Kbit/sec)** – Sets the rate limit level. (Range: 0 - 1048544 Kbps in steps of 16)

WEB INTERFACE

To configure bandwidth control:

1. Click Configuration, Bandwidth Control.
2. Select the ports to configure.
3. Set Type to Ingress or Egress .
4. Set State to Enable.
5. Configure the maximum rate allowed on the ports.
6. Click Apply.

Figure 34: Bandwidth Control



17 JUMBO FRAME

The switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames up to 9216 bytes. Compared to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields.

USAGE GUIDELINES

To use jumbo frames, both the source and destination end nodes (such as a computer or server) must support this feature. Also, when the connection is operating at full duplex, all switches in the network between the two end nodes must be able to accept the extended frame size. And for half-duplex connections, all devices in the collision domain would need to support jumbo frames.

PARAMETERS

The following parameter is displayed on the Jumbo Frame page:

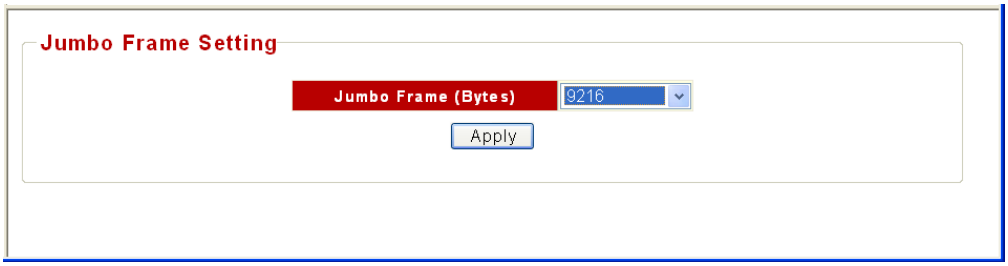
- **Jumbo Frame (Bytes)** — Configures support for jumbo frames. (Options: 9216, 1522, 1536, 1552 Bytes; Default: 9216 bytes)

WEB INTERFACE

To configure Jumbo Frames:

1. Click Configuration, Jumbo Frame.
2. Select the frame size to configure.
3. Click Apply.

Figure 35: Jumbo Frame Setting



18 MANAGEMENT ACCESS FILTER

You can create a list of up to eight IP addresses or IP address groups that are allowed management access to the switch through the web interface.

USAGE GUIDELINES

- The web management interface is open to all IP addresses by default. Once you add an entry to a filter list, access to that interface is restricted to the specified addresses.
- If anyone tries to access a management interface on the switch from an invalid address, the switch will reject the connection, enter an event message in the system log.
- When entering addresses, the switch will not accept overlapping address ranges.
- You cannot delete an individual address from a specified range. You must delete the entire range, and reenter the addresses.

PARAMETERS

The following parameters are displayed on the Management Access Filter page:

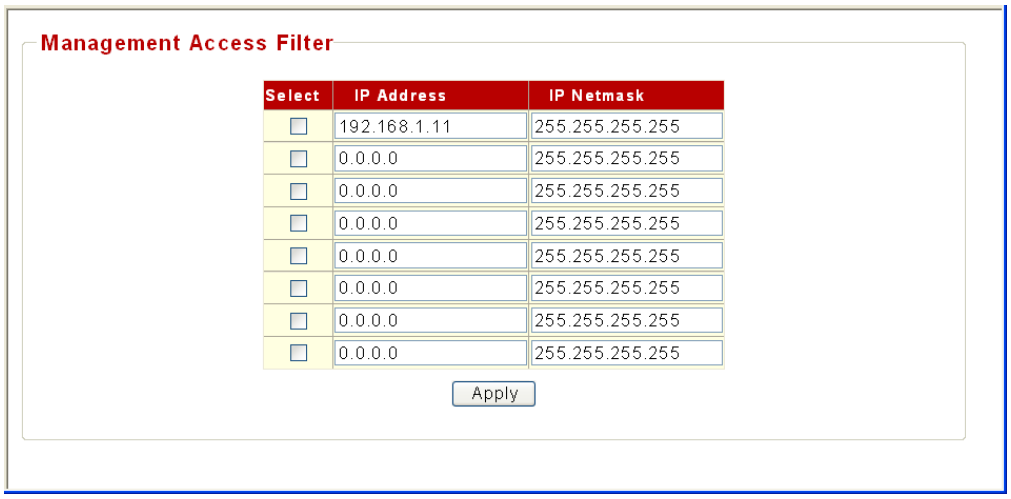
- **IP Address** — An IP address, or an address specifying a range, that is allowed management access to the switch.
- **IP Netmask** — A mask that specifies a single IP address, or defines a range of IP addresses. (Default: 255.255.255.255 for a single IP address)

WEB INTERFACE

To configure Management Access Filters:

1. Click Configuration, Management Access Filter.
2. Enter an IP address
3. Specify a netmask to define a single IP address, or an address range.
4. Select the table entry to activate the filter.
5. Click Apply.

Figure 36: Management Access Filter



19 MAC ADDRESS SECURITY

This chapter includes the following sections for configuring MAC address security:

- "MAC Forwarding Table" on page 105
- "Static MAC Addresses" on page 106
- "MAC Address Filtering" on page 107

MAC FORWARDING TABLE

Switches store the addresses for all known devices. This information is used to pass traffic directly between the inbound and outbound ports. All the addresses learned by monitoring traffic are stored in the dynamic address table. You can also manually configure static addresses that are bound to a specific port.

The Dynamic Address Table contains the MAC addresses learned by monitoring the source address for traffic entering the switch. When the destination address for inbound traffic is found in the database, the packets intended for that address are forwarded directly to the associated port. Otherwise, the traffic is flooded to all ports.

PARAMETERS

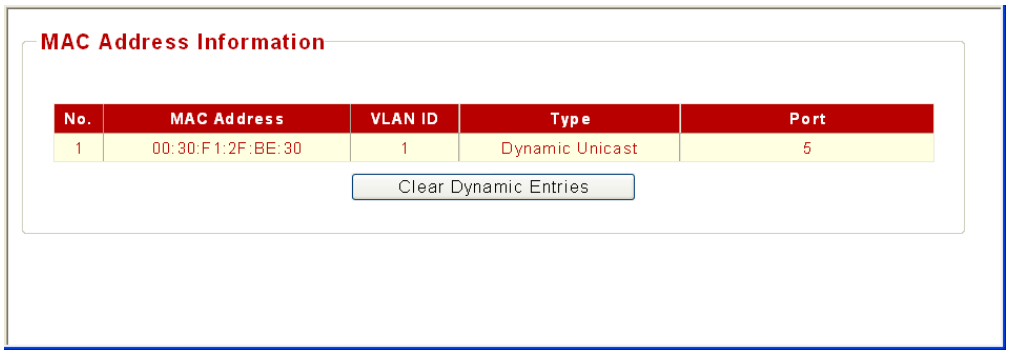
The following parameters are displayed on the MAC Forwarding Table page:

- **No.** — The number of the address entry in the forwarding table.
- **MAC Address** — Physical address associated with this interface.
- **VLAN ID** — The ID of a configured VLAN (1-4094).
- **Type** — Indicates if the MAC address has been dynamically learned or configured as a static entry.
- **Port** — Indicates the port.
- **Clear Dynamic Entries** — Removes all dynamically learned addresses from the forwarding table.

WEB INTERFACE

To display the MAC address forwarding table, click Security, MAC Address, MAC Forwarding Table.

Figure 37: MAC Address Forwarding Table



STATIC MAC ADDRESSES

A static address can be assigned to a specific interface on the switch. Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.

PARAMETERS

The following parameters are displayed on the Static MAC page:

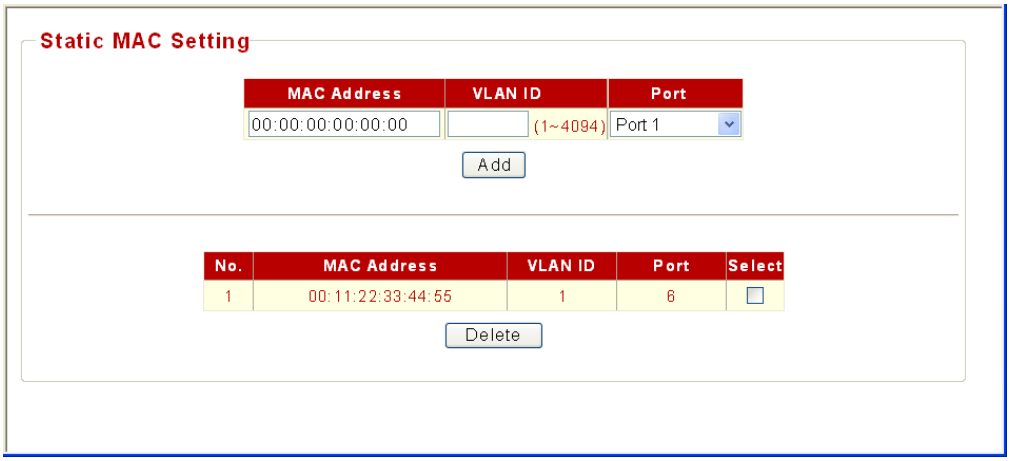
- **MAC Address** — Physical address of a device mapped to an interface.
- **VLAN ID** — The ID of a configured VLAN (1-4094).
- **Port** — Port or trunk associated with the device that is assigned as a static address.

WEB INTERFACE

To configure static MAC addresses:

1. Click Security, MAC Address, Static MAC.
2. Specify the MAC address to be statically assigned.
3. Specify the VLAN ID.
4. Select the port or trunk interface for the static assignment.
5. Click Add.

Figure 38: Static MAC Setting



MAC ADDRESS FILTERING

The MAC Filtering pages are used to filter service to clients attempting to access the Internet based on protocol type, destination/source MAC address, and the direction of traffic for each packet.

Click Advanced Setup, Security, MAC Filtering. If a policy has been set, you can change the filtering action to Forwarded or Blocked. To add a new policy, click Add. To remove a policy, mark the "Remove" check box next to the required entry, and click Remove.

PARAMETERS

The following parameters are displayed on the MAC Address Filtering page:

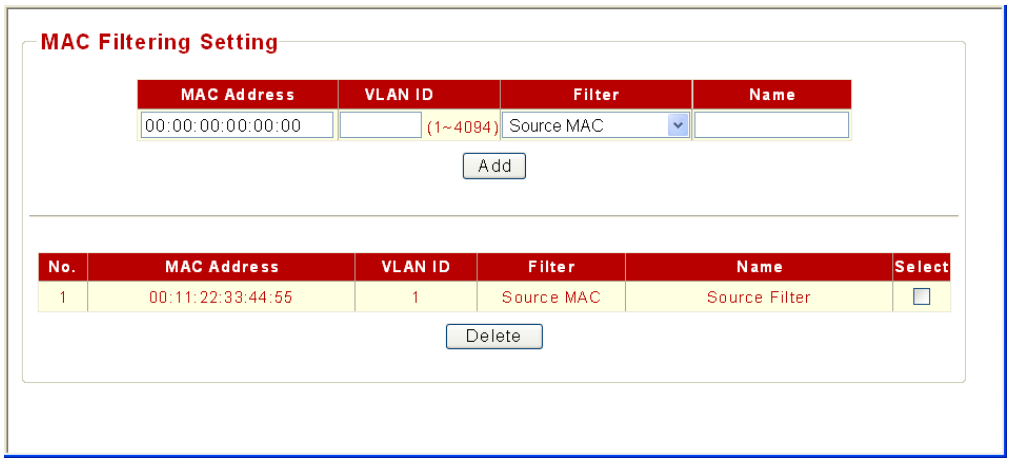
- **MAC Address** — Physical address of a device.
- **VLAN ID** — The ID of a configured VLAN (1-4094).
- **Filter** — Filters traffic matching the MAC address in packets. (Options: Source MAC, Destination MAC, Both; Default: Source MAC)
  - **Destination MAC** — Filters packets with a matching destination MAC address.
  - **Source MAC** — Filters packets with a matching source MAC address.
  - **Both** — Filters packets with a matching the source or destination MAC address.
- **Name** – A descriptive name for the MAC address filter.

WEB INTERFACE

To configure MAC Address Filtering:

1. Click Security, MAC Address, MAC Address Filtering.
2. Specify the MAC address to be filtered.
3. Specify the VLAN ID.
4. Select to filter the MAC address as the source, destination, or both.
5. Set a name to describe the filter.
6. Click Add.

Figure 39: MAC Address Filtering



20 802.1X SECURITY

This chapter includes the following sections for configuring 802.1X security:

- "Configuring 802.1X Authentication" on page 109
- "802.1X Global Settings" on page 110
- "802.1X Port Settings" on page 111

CONFIGURING 802.1X AUTHENTICATION

Network switches can provide open and easy access to network resources by simply attaching a client PC. Although this automatic configuration and access is a desirable feature, it also allows unauthorized personnel to easily intrude and possibly gain access to sensitive network data.

The IEEE 802.1X (802.1X or dot1x) standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. Access to all switch ports in a network can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

This switch uses the Extensible Authentication Protocol over LANs (EAPOL) to exchange authentication protocol messages with the client, and a remote RADIUS authentication server to verify user identity and access rights. When a client (Supplicant) connects to a switch port, the switch (Authenticator) responds with an EAPOL identity request. The client provides its identity (such as a user name) in an EAPOL response to the switch, which it forwards to the RADIUS server. The RADIUS server verifies the client identity and sends an access challenge back to the client. The EAP packet from the RADIUS server contains not only the challenge, but the authentication method to be used. The client can reject the authentication method and request another, depending on the configuration of the client software and the RADIUS server. The client responds to the appropriate method with its credentials, such as a password or certificate. The RADIUS server verifies the client credentials and responds with an accept or reject packet. If authentication is successful, the switch allows the client to access the network. Otherwise, non-EAP traffic on the port is blocked.

The operation of 802.1X on the switch requires the following:

- The switch must have an IP address assigned.

- RADIUS authentication must be enabled on the switch and the IP address of the RADIUS server specified.
- 802.1X must be enabled globally for the switch.
- Each switch port that will be used must be set to "Authentication" mode.
- Each client that needs to be authenticated must have dot1X client software installed and properly configured.
- The RADIUS server and client also have to support the same EAP authentication type.

802.1X GLOBAL SETTINGS

The 802.1X protocol provides port authentication. The 802.1X protocol must be enabled globally for the switch system before port settings are active.

PARAMETERS

The following parameters are displayed on the 802.1X Setting page:

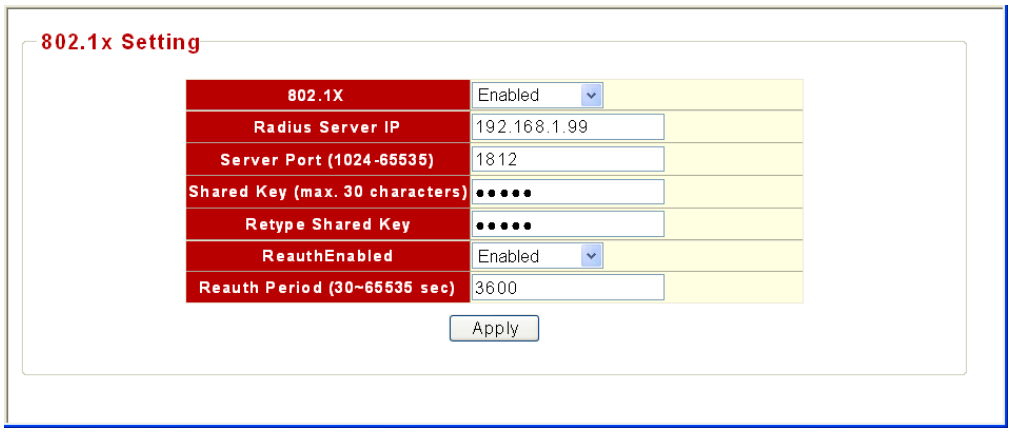
- **802.1X** — Sets the global setting for 802.1X. (Default: Disabled)
- **RADIUS Server IP** — Address of the authentication server.
- **Server Port** — Network (UDP) port of RADIUS server used for authentication messages. (Range: 1024-65535; Default: 1812)
- **Shared Key** — Encryption key used for RADIUS server messages. Do not use blank spaces in the string. (Maximum length: 30 characters)
- **Retype Shared Key** — Re-type the string entered in the previous field to ensure no errors were made. The switch will not change the encryption key if these two fields do not match.
- **ReauthEnabled** — Sets clients to be re-authenticated after the interval specified by the Reauth Period. Re-authentication can be used to detect if a new device is plugged into a switch port. (Default: Enabled)
- **Reauth Period** — Sets the time period after which a connected client must be re-authenticated. (Range: 30-65535 seconds; Default: 3600 seconds)

WEB INTERFACE

To configure 802.1X global settings:

1. Click Security, 802.1X, 802.1X Setting.
2. Set 802.1X to Enabled.
3. Specify the RADIUS server IP address.
4. Specify the RADIUS server shared key.
5. Modified other parameters as required.
6. Click Apply.

Figure 40: 802.1X Setting



802.1X PORT SETTINGS

When 802.1X is enabled, you need to configure the parameters for the authentication process that runs between the client and the switch (that is, authenticator), as well as the client identity lookup process that runs between the switch and authentication server. These parameters are described in this section.

PARAMETERS

The following parameters are displayed on the 802.1X Port Setting page:

- **Port** – Port number.
- **Mode** – Sets the authentication mode to one of the following options:
  - **Authentication** – Requires a dot1x-aware client to be authorized by the authentication server. Clients that are not dot1x-aware will be denied access.

- **Force-Authorized** – Forces the port to grant access to all clients, either dot1x-aware or otherwise.
- **Force-Unauthorized** – Forces the port to deny access to all clients, either dot1x-aware or otherwise.
- **No Authentication** – Disables 802.1X authentication on the port. (This is the default setting.)

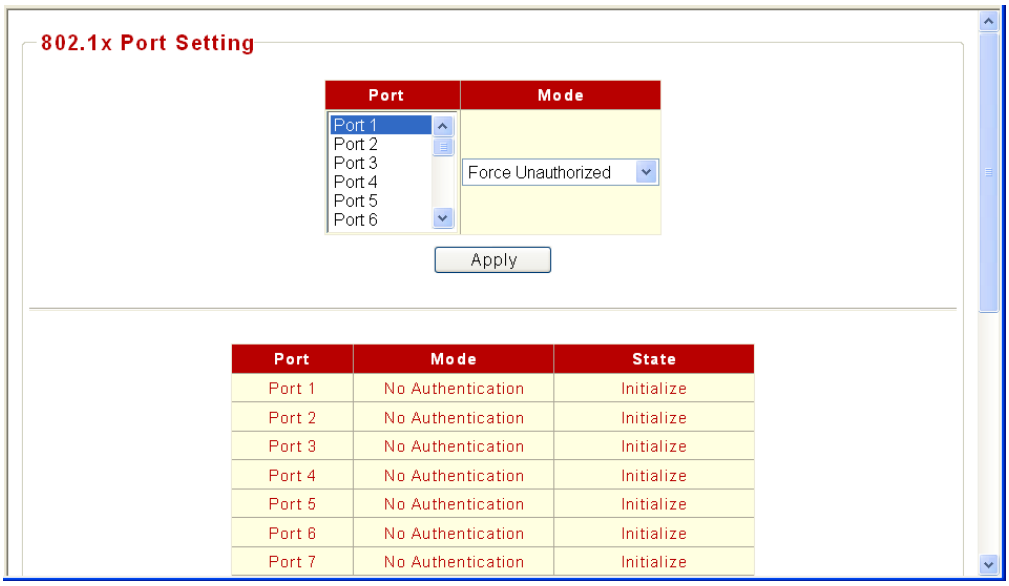
- **State** — Shows the current status of the 802.1X authentication process.

WEB INTERFACE

To configure 802.1X port settings:

1. Click Security, 802.1X, 802.1X Port Setting.
2. Select one or more ports to configure.
3. Set the 802.1X Mode to "Authentication."
4. Click Apply.

Figure 41: 802.1X Port Setting



21 GENERAL SECURITY SETTINGS

This chapter includes the following sections for other general security settings:

- "IP Filter Security" on page 113
- "Storm Control Setting" on page 114
- "Port Isolation" on page 116
- "Defence Engine" on page 117

IP FILTER SECURITY

IP Filter Security is a feature that filters IP traffic on port interfaces based on manually configured entries in the IP Filter table, or allowed IP address assignment through DHCP. IP Filter Security can be used to prevent traffic attacks caused when a host tries to use the IP address of a neighbor to access the network.

PARAMETERS

The following parameters are displayed on the IP Filter Setting page:

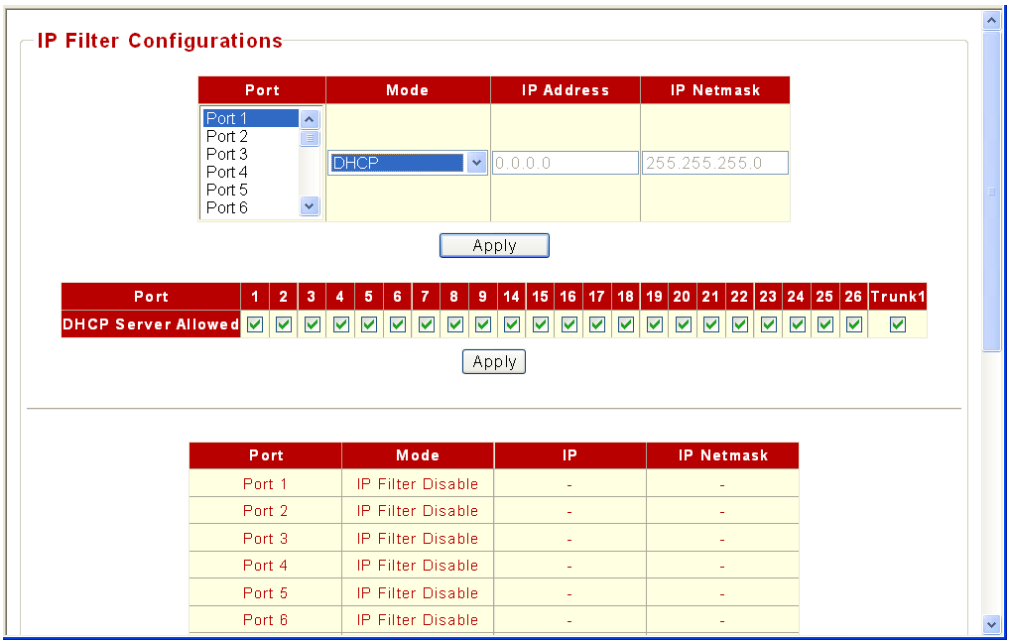
- **Port** – Port number.
- **Mode** – Configures the switch to filter traffic based on IP addresses. (Default: IP Filter Disable)
  - **IP Filter Disable** – Disables IP filtering on the port.
  - **Static** – Enables traffic filtering based on IP addresses configured in the table.
  - **DHCP** – Enables traffic filtering based on IP addresses assigned through DHCP.
- **IP Address** — An IP address, or an address specifying a range, that is allowed access through the switch.
- **IP Netmask** — A mask that specifies a single IP address, or defines a range of IP addresses. (Default: 255.255.255.0)
- **DHCP Server Allowed** — Permits traffic from a DHCP server through the specified ports. (Default: All ports allowed)

WEB INTERFACE

To configure IP Filter settings:

1. Click Security, IP Filter Setting.
2. Select one or more ports to configure.
3. Select the mode Static and set an IP address, or select DHCP.
4. Select ports on which to allow traffic to DHCP servers.
5. Click Apply.

Figure 42: IP Filter Setting



STORM CONTROL SETTING

Broadcast storms may occur when a device on your network is malfunctioning, or if application programs are not well designed or properly configured. If there is too much broadcast traffic on your network, performance can be severely degraded or everything can come to complete halt.

You can protect your network from broadcast storms by setting a threshold for broadcast traffic. Any broadcast packets exceeding the specified threshold will then be dropped.

You can also protect your network from excess multicast or unknown multicast/unicast traffic traffic by setting thresholds for each port. Any packets exceeding the specified threshold will then be dropped.

PARAMETERS

The following parameters are displayed on the Storm Control page:

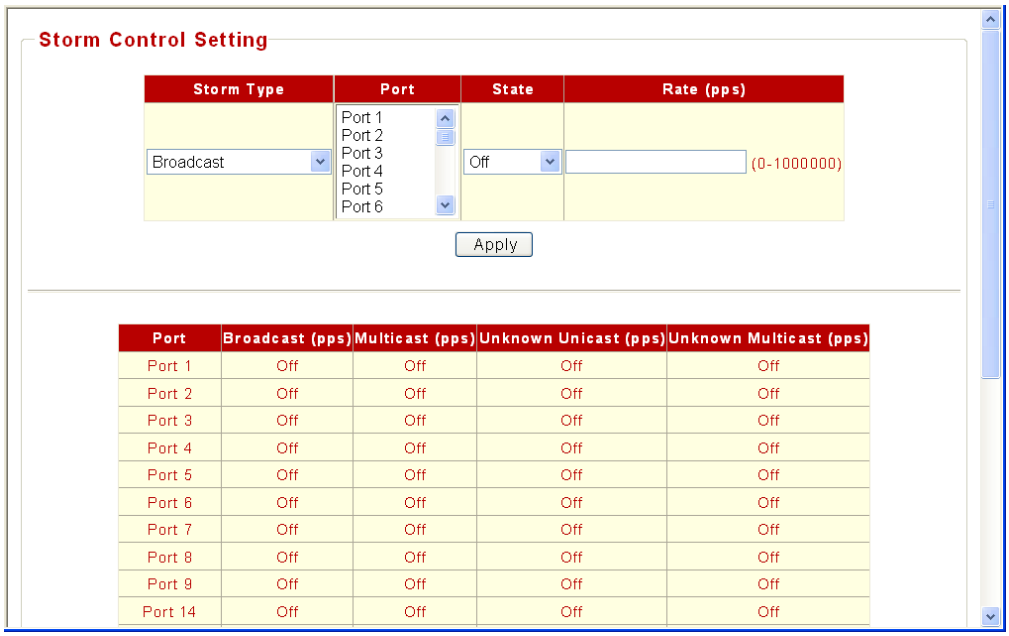
- **Storm Type** — Selects the storm control type. (Broadcast, Multicast, Unknown Unicast, Unknown Multicast)
- **Port** — Selects port and trunk interfaces. (Port Range: 1-26)
- **State** — Enables or disables storm control. (Default: Off)
- **Rate** — Threshold as packets per second (pps). (Range: 0-1000000)

WEB INTERFACE

To configure Storm Control settings:

1. Click Security, Storm Control.
2. Select the Storm Control type.
3. Select one or more ports to configure.
4. Set the State to "On" and set the threshold rate.
5. Click Apply.

Figure 43: Storm Control Settings



PORT ISOLATION

Port Isolation provides port-based security and isolation of local ports. The switch isolates port traffic by specifying those ports to which it can forward or receive traffic.

PARAMETERS

The following parameters are displayed on the Port Isolation page:

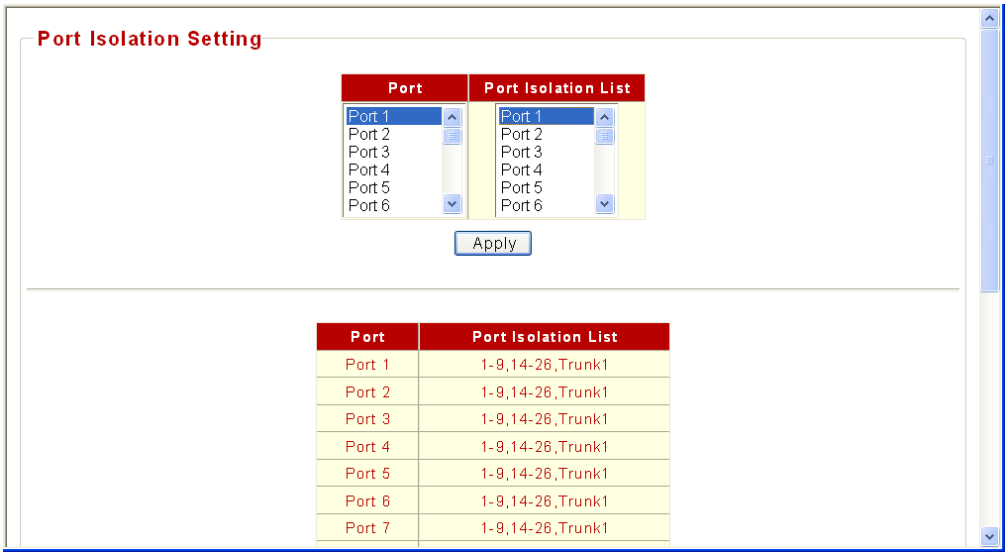
- **Port** — Selects port and trunk interfaces. (Port Range: 1-26)
- **Port Isolation List** — Selects port and trunk interfaces to which traffic can be forwarded and received. (Port Range: 1-26; Default: All ports and trunks)

WEB INTERFACE

To configure Port Isolation settings:

1. Click Security, Port Isolation.
2. Select one or more ports to configure.
3. Select one or more ports to which traffic can be forwarded and received.
4. Click Apply.

Figure 44: Port Isolation Settings



DEFENCE ENGINE

Defence Engine is a advanced feature that can prevent switch's CPU from being overwhelmed by flooded packets, such as unknown unicast, unknown multicast, or broadcast packets. This function can be used to prevent malicious viruses or worm attacks.

PARAMETERS

The following parameter is displayed on the Defence Engine page:

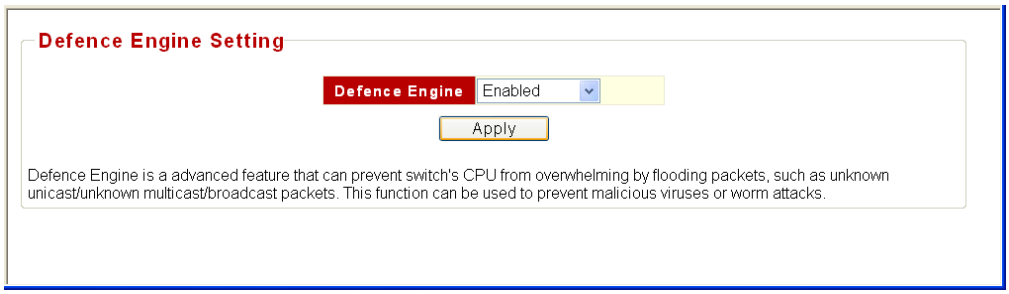
- **Defence Engine** — Enables or disables the feature. (Default: Enabled)

WEB INTERFACE

To configure Defence Engine settings:

1. Click Security, Defence Engine.
2. Set Defence Engine status to Enabled.
3. Click Apply.

Figure 45: Defence Engine Setting


Defence Engine Setting
Defence Engine
Enabled
Apply
Defence Engine is a advanced feature that can prevent switch's CPU from overwhelming by flooding packets, such as unknown unicast/unknown multicast/broadcast packets. This function can be used to prevent malicious viruses or worm attacks.

22 PORT STATISTICS

You can display standard statistics on network traffic passing through each port. This information can be used to identify potential problems with the switch (such as a faulty port or unusually heavy loading).

All values displayed have been accumulated since the last system reboot.

PARAMETERS

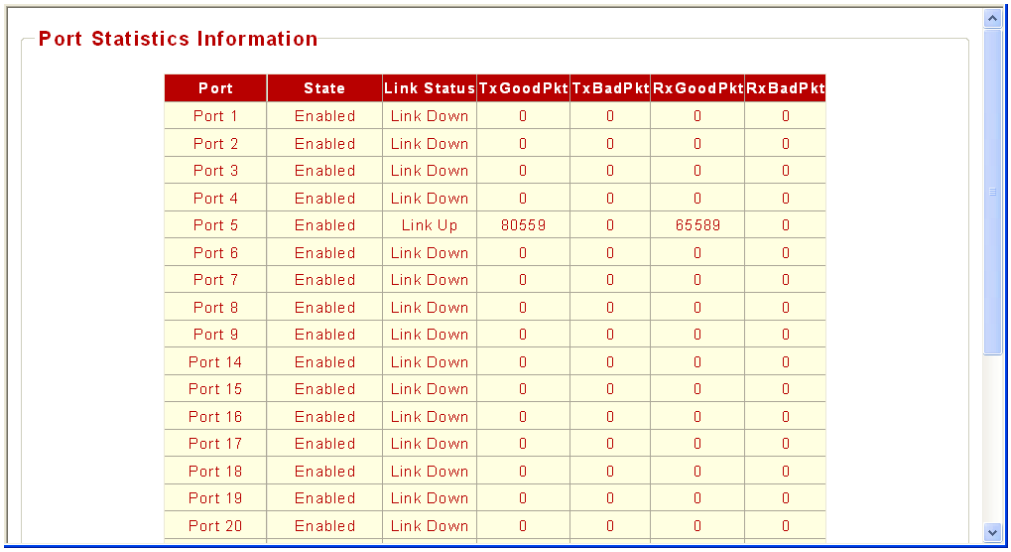
The following parameters are displayed on the Port Statistics Information page:

- **Port** — The port number.
- **State** — Displays the link state of port interfaces (Enabled or Disabled).
- **Link Status** — Displays the link state of the port interface (Link Up or Link Down).
- **TxGoodPkt** — The total number of packets transmitted out of the interface.
- **TxBadPkt** — The total number of outbound packets that could not be transmitted because of errors.
- **RxGoodPkt** — The total number of packets received on the interface.
- **RxBadPkt** — The total number of inbound packets that contained errors preventing them from being deliverable.
- **Clear** — Click the button to reset all counters.

WEB INTERFACE

To display port statistics, click Monitoring, Port Statistics.

Figure 46: Port Statistics



Port	State	Link Status	TxGoodPkt	TxBadPkt	RxGoodPkt	RxBadPkt
Port 1	Enabled	Link Down	0	0	0	0
Port 2	Enabled	Link Down	0	0	0	0
Port 3	Enabled	Link Down	0	0	0	0
Port 4	Enabled	Link Down	0	0	0	0
Port 5	Enabled	Link Up	80559	0	65589	0
Port 6	Enabled	Link Down	0	0	0	0
Port 7	Enabled	Link Down	0	0	0	0
Port 8	Enabled	Link Down	0	0	0	0
Port 9	Enabled	Link Down	0	0	0	0
Port 14	Enabled	Link Down	0	0	0	0
Port 15	Enabled	Link Down	0	0	0	0
Port 16	Enabled	Link Down	0	0	0	0
Port 17	Enabled	Link Down	0	0	0	0
Port 18	Enabled	Link Down	0	0	0	0
Port 19	Enabled	Link Down	0	0	0	0
Port 20	Enabled	Link Down	0	0	0	0

23 MANAGEMENT TOOLS

This chapter includes the following sections for management tools:

- "HTTP Upgrade" on page 121
- "Restoring Factory Defaults" on page 122
- "Resetting the Switch" on page 123

HTTP UPGRADE

Use the HTTP Upgrade page to upgrade the switch's system firmware by specifying a new software file. You can also use the HTTP Upgrade page to save the current configuration to a file on your computer, or to restore previously saved configuration settings to the switch.

PARAMETERS

The following parameters are displayed on the HTTP Upgrade page:

- **HTTP Configuration Backup** — Click the Backup button to save the current configuration settings to a file on the local web management station.
- **HTTP Configuration Restore** — Restores previously saved configuration settings to the switch from a file on the local web management station. Use the Browse button to locate the configuration file, then click Restore.
- **HTTP Firmware Upgrade** — Upgrades the switch software from a file on the local web management station. Use the Browse button to locate the software file, then click Upgrade.

WEB INTERFACE

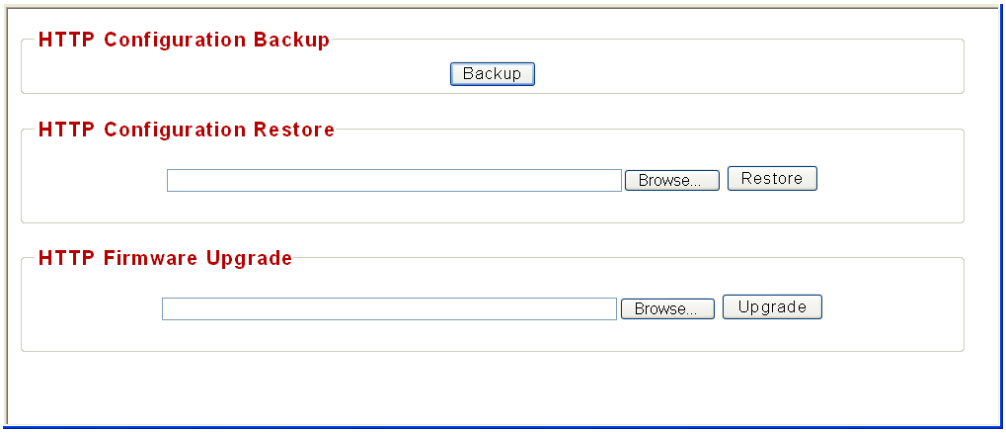
To upgrade switch software:

1. Click Tools, HTTP Upgrade.
2. Click the Browse button, and select the firmware file.
3. Click the Upgrade button to upgrade the switch's firmware.

After the software file is uploaded, the switch prompts for a reboot.

CAUTION: Do not reset or power off the switch during the upgrade process or the switch may fail to function afterwards.

Figure 47: Software Upgrade



RESTORING FACTORY DEFAULTS

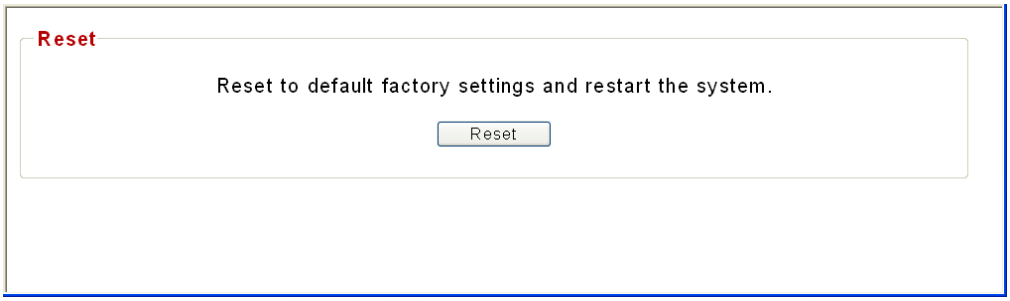
Use the Reset page to restore the original factory settings. Note that the LAN IP Address, Subnet Mask and Gateway IP Address will be reset to their factory defaults.

WEB INTERFACE

To restore factory defaults, click Tools, Reset, then click the Reset button.

The reset will be complete when the web interface displays the login page.

Figure 48: Restoring Factory Defaults



RESETTING THE SWITCH

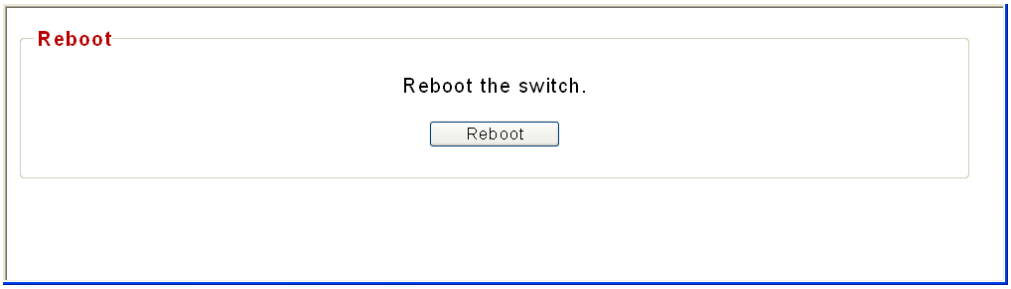
Use the Reboot page to restart the switch.

WEB INTERFACE

To restart the switch, click Tools, Reboot, then click the Reboot button.

The reboot will be complete when the web interface displays the login page.

Figure 49: Reboot Switch



Section III

Appendices

This section provides additional information and includes these items:

- "Software Specifications" on page 127
- "Troubleshooting" on page 131

A SOFTWARE SPECIFICATIONS

SOFTWARE FEATURES

AUTHENTICATION	Local, RADIUS, Port (802.1X), HTTPS, Port Security, IP Filter
PORT CONFIGURATION	1000BASE-T: 10/100 Mbps at half/full duplex, 1000 Mbps at full duplex 1000BASE-BX/SX/LX/LH - 1000 Mbps at full duplex (SFP)
FLOW CONTROL	Full Duplex: IEEE 802.3-2005 Half Duplex: Back pressure
STORM CONTROL	Broadcast, multicast, or unicast traffic throttled above a critical threshold
PORT MIRRORING	Multiple source ports, one destination port
RATE LIMITS	Input/ouput limit per port
PORT TRUNKING	Static trunks (Cisco EtherChannel compliant) Dynamic trunks (Link Aggregation Control Protocol)
SPANNING TREE ALGORITHM	Spanning Tree Protocol (STP, IEEE 802.1D-2004) Rapid Spanning Tree Protocol (RSTP, STP, IEEE 802.1D-2004)
VLAN SUPPORT	Up to 256 groups; port-based, or tagged (802.1Q) VLAN Stacking (QinQ)
CLASS OF SERVICE	Supports four levels of priority Strict, Weighted Fair Queueing, or Weighted Round Robin queueing Queue mode and CoS configured by port or DSCP Layer 3/4 priority mapping: IP DSCP remarking

MULTICAST FILTERING IGMP Snooping

ADDITIONAL FEATURES DHCP Client
LLDP (Link Layer Discover Protocol)
SNMP (Simple Network Management Protocol)

MANAGEMENT FEATURES

IN-BAND MANAGEMENT Web-based HTTP or SNMP manager

SNMP Management access via MIB database
Trap management to specified hosts

STANDARDS

IEEE 802.1AB Link Layer Discovery Protocol
IEEE 802.1D-2004 Spanning Tree Algorithm and traffic priorities
  Spanning Tree Protocol
  Rapid Spanning Tree Protocol
IEEE 802.1p Priority tags
IEEE 802.1Q VLAN
IEEE 802.1X Port Authentication
IEEE 802.3-2005
  Ethernet, Fast Ethernet, Gigabit Ethernet
  Link Aggregation Control Protocol (LACP)
IEEE 802.3ac VLAN tagging
ARP (RFC 826)
DHCP Client (RFC 2131)
ICMP (RFC 792)
IGMP (RFC 1112)
IGMPv2 (RFC 2236)
IGMPv3 (RFC 3376) - partial support
RADIUS+ (RFC 2618)
SNMP (RFC 1157)
SNMPv2c (RFC 2571)

MANAGEMENT INFORMATION BASES

Bridge MIB (RFC 1493)
Differentiated Services MIB (RFC 3289)
Entity MIB (RFC 2737)
Ether-like MIB (RFC 2665)
Extended Bridge MIB (RFC 2674)
Extensible SNMP Agents MIB (RFC 2742)
Forwarding Table MIB (RFC 2096)
IGMP MIB (RFC 2933)
Interface Group MIB (RFC 2233)
Interfaces Evolution MIB (RFC 2863)
IP MIB (RFC 2011)
IP Multicasting related MIBs
IPV6-MIB (RFC 2065)
IPV6-ICMP-MIB (RFC 2066)
IPV6-TCP-MIB (RFC 2052)
IPV6-UDP-MIB (RFC2054)
MAU MIB (RFC 3636)
MIB II (RFC 1213)
Port Access Entity MIB (IEEE 802.1X)
Port Access Entity Equipment MIB
Private MIB
RADIUS Authentication Client MIB (RFC 2621)
SNMPv2 IP MIB (RFC 2011)
TCP MIB (RFC 2012)
Trap (RFC 1215)
UDP MIB (RFC 2013)

B TROUBLESHOOTING

PROBLEMS ACCESSING THE MANAGEMENT INTERFACE

Table 11: Troubleshooting Chart

Symptom	Action
Cannot connect using a web browser or SNMP software	◆ Be sure the switch is powered up. ◆ Check network cabling between the management station and the switch. ◆ Check that you have a valid network connection to the switch and that the port you are using has not been disabled. ◆ Be sure you have configured the VLAN interface through which the management station is connected with a valid IP address, subnet mask and default gateway. ◆ Be sure the management station has an IP address in the same subnet as the switch's IP interface to which it is connected.
Forgot or lost the password	◆ Contact your local distributor.

GLOSSARY

ACL Access Control List. ACLs can limit network traffic and restrict access to certain users or devices by checking each packet for certain IP or MAC (i.e., Layer 2) information.

BOOTP Boot Protocol. BOOTP is used to provide bootup information for network devices, including IP address information, the address of the TFTP server that contains the devices system files, and the name of the boot file.

CoS Class of Service is supported by prioritizing packets based on the required level of service, and then placing them in the appropriate output queue. Data is transmitted from the queues using weighted round-robin service to enforce priority service and prevent blockage of lower-level queues. Priority may be set according to the port default, the packet's priority bit (in the VLAN tag), TCP/UDP port number, IP Precedence bit, or DSCP priority bit.

DIFFSERV Differentiated Services provides quality of service on large networks by employing a well-defined set of building blocks from which a variety of aggregate forwarding behaviors may be built. Each packet carries information (DS byte) used by each hop to give it a particular forwarding treatment, or per-hop behavior, at each network node. DiffServ allocates different levels of service to users on the network with mechanisms such as traffic meters, shapers/droppers, packet markers at the boundaries of the network.

DHCP Dynamic Host Control Protocol. Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

DHCP OPTION 82 A relay option for sending information about the requesting client (or an intermediate relay agent) in the DHCP request packets forwarded by the switch and in reply packets sent back from the DHCP server. This information can be used by DHCP servers to assign fixed IP addresses, or set other services or policies for clients.

DNS Domain Name Service. A system used for translating host names for network nodes into IP addresses.

DSCP Differentiated Services Code Point Service. DSCP uses a six-bit tag to provide for up to 64 different forwarding behaviors. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP bits are mapped to the Class of Service categories, and then into the output queues.

EUI Extended Universal Identifier is an address format used by IPv6 to identify the host portion of the network address. The interface identifier in EUI compatible addresses is based on the link-layer (MAC) address of an interface. Interface identifiers used in global unicast and other IPv6 address types are 64 bits long and may be constructed in the EUI-64 format. The modified EUI-64 format interface ID is derived from a 48-bit link-layer address by inserting the hexadecimal number FFFE between the upper three bytes (OUI field) and the lower 3 bytes (serial number) of the link layer address. To ensure that the chosen address is from a unique Ethernet MAC address, the 7th bit in the high-order byte is set to 1 (equivalent to the IEEE Global/Local bit) to indicate the uniqueness of the 48-bit address.

EAPOL Extensible Authentication Protocol over LAN. EAPOL is a client authentication protocol used by this switch to verify the network access rights for any device that is plugged into the switch. A user name and password is requested by the switch, and then passed to an authentication server (e.g., RADIUS) for verification. EAPOL is implemented as part of the IEEE 802.1X Port Authentication standard.

GARP Generic Attribute Registration Protocol. GARP is a protocol that can be used by endstations and switches to register and propagate multicast group membership information in a switched environment so that multicast data frames are propagated only to those parts of a switched LAN containing registered endstations. Formerly called Group Address Registration Protocol.

GMRP Generic Multicast Registration Protocol. GMRP allows network devices to register end stations with multicast groups. GMRP requires that any participating network devices or end stations comply with the IEEE 802.1p standard.

GVRP GARP VLAN Registration Protocol. Defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports along the Spanning Tree so that VLANs defined in each switch can work automatically over a Spanning Tree network.

IEEE 802.1D Specifies a general method for the operation of MAC bridges, including the Spanning Tree Protocol.

IEEE 802.1Q VLAN Tagging—Defines Ethernet frame tags which carry VLAN information. It allows switches to assign endstations to different virtual LANs, and defines a standard way for VLANs to communicate across switched networks.

IEEE 802.1P An IEEE standard for providing quality of service (QoS) in Ethernet networks. The standard uses packet tags that define up to eight traffic classes and allows switches to transmit packets based on the tagged priority value.

IEEE 802.1W An IEEE standard for the Rapid Spanning Tree Protocol (RSTP) which reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard. (Now incorporated in IEEE 802.1D-2004)

IEEE 802.1X Port Authentication controls access to the switch ports by requiring users to first enter a user ID and password for authentication.

IEEE 802.3AC Defines frame extensions for VLAN tagging.

IEEE 802.3X Defines Ethernet frame start/stop requests and timers used for flow control on full-duplex links. (Now incorporated in IEEE 802.3-2002)

IGMP Internet Group Management Protocol. A protocol through which hosts can register with their local router for multicast services. If there is more than one multicast switch/router on a given subnetwork, one of the devices is made the "querier" and assumes responsibility for keeping track of group membership.

IGMP QUERY On each subnetwork, one IGMP-capable device will act as the querier — that is, the device that asks all hosts to report on the IP multicast groups they wish to join or to which they already belong. The elected querier will be the device with the lowest IP address in the subnetwork.

IGMP SNOOPING Listening to IGMP Query and IGMP Report packets transferred between IP Multicast Routers and IP Multicast host groups to identify IP Multicast group members.

IN-BAND MANAGEMENT Management of the network from a station attached directly to the network.

IP MULTICAST FILTERING A process whereby this switch can pass multicast traffic along to participating hosts.

IP PRECEDENCE The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight different priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. The eight values are mapped one-to-one to the Class of Service categories by default, but may be configured differently to suit the requirements for specific network applications.

LACP Link Aggregation Control Protocol. Allows ports to automatically negotiate a trunked link with LACP-configured ports on another device.

LAYER 2 Data Link layer in the ISO 7-Layer Data Communications Protocol. This is related directly to the hardware interface for network devices and passes on traffic based on MAC addresses.

LINK AGGREGATION *See Port Trunk.*

MD5 MD5 Message-Digest is an algorithm that is used to create digital signatures. It is intended for use with 32 bit machines and is safer than the MD4 algorithm, which has been broken. MD5 is a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest.

MIB Management Information Base. An acronym for Management Information Base. It is a set of database objects that contains information about a specific device.

MULTICAST SWITCHING A process whereby the switch filters incoming multicast frames for services for which no attached host has registered, or forwards them to all ports contained within the designated multicast VLAN group.

MVR Multicast VLAN Registration is a method of using a single network-wide multicast VLAN to transmit common services, such as such as television channels or video-on-demand, across a service-provider's network. MVR simplifies the configuration of multicast services by using a common VLAN for distribution, while still preserving security and data isolation for subscribers residing in both the MVR VLAN and other standard or private VLAN groups.

NTP Network Time Protocol provides the mechanisms to synchronize time across the network. The time servers operate in a hierarchical-master-slave configuration in order to synchronize local clocks within the subnet and to national time standards via wire or radio.

PORT AUTHENTICATION *See IEEE 802.1X*.

PORT MIRRORING A method whereby data on a target port is mirrored to a monitor port for troubleshooting with a logic analyzer or RMON probe. This allows data on the target port to be studied unobstructively.

PORT TRUNK Defines a network link aggregation and trunking method which specifies how to create a single high-speed logical link that combines several lower-speed physical links.

PRIVATE VLANS Private VLANs provide port-based security and isolation between ports within the assigned VLAN. Data traffic on downlink ports can only be forwarded to, and from, uplink ports.

QOS Quality of Service. QoS refers to the capability of a network to provide better service to selected traffic flows using features such as data prioritization, queuing, congestion avoidance and traffic shaping. These features effectively provide preferential treatment to specific flows either by raising the priority of one flow or limiting the priority of another flow.

RADIUS Remote Authentication Dial-in User Service. RADIUS is a logon authentication protocol that uses software running on a central server to control access to RADIUS-compliant devices on the network.

RSTP Rapid Spanning Tree Protocol. RSTP reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard.

SNMP Simple Network Management Protocol. The application protocol in the Internet suite of protocols which offers network management services.

SNTP Simple Network Time Protocol allows a device to set its internal clock based on periodic updates from a Network Time Protocol (NTP) server. Updates can be requested from a specific NTP server, or can be received via broadcasts sent by NTP servers.

SSH Secure Shell is a secure replacement for remote access functions, including Telnet. SSH can authenticate users with a cryptographic key, and encrypt data connections between management clients and the switch.

STA Spanning Tree Algorithm is a technology that checks your network for any loops. A loop can often occur in complicated or backup linked network systems. Spanning Tree detects and directs data along the shortest available path, maximizing the performance and efficiency of the network.

TCP/IP Transmission Control Protocol/Internet Protocol. Protocol suite that includes TCP as the primary transport protocol, and IP as the network layer protocol.

TELNET Defines a remote communication facility for interfacing to a terminal device over TCP/IP.

TFTP Trivial File Transfer Protocol. A TCP/IP protocol commonly used for software downloads.

UDP User Datagram Protocol. UDP provides a datagram mode for packet-switched communications. It uses IP as the underlying transport mechanism to provide access to IP-like services. UDP packets are delivered just like IP packets – connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.

UTC Universal Time Coordinate. UTC is a time scale that couples Greenwich Mean Time (based solely on the Earth's rotation rate) with highly accurate atomic time. The UTC does not have daylight saving time.

VLAN Virtual LAN. A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, and allows users to share information and resources as though located on the same LAN.

INDEX

NUMERICS

802.1Q tunnel
    mode selection 63
802.1X
    port authentication 109

B

BPDU 72

C

community string 92

D

default settings, system 21

E

edge port, STA 75, 76

F

firmware
    displaying version 37

I

IEEE 802.1D 72
IEEE 802.1X 109
IGMP 65
    fast leave, status 68
    snooping 65
    snooping, fast leave 68
IPv4 address setting 40

L

LACP
    configuration 54
    local parameters 54
    protocol parameters 54
Link Aggregation Control Protocol *See* LACP
Link Layer Discovery Protocol *See* LLDP
link type, STA 76
LLDP 87
    TLV 87
log-in, web interface 32

M

main menu 33
Management Information Bases (MIBs) 129
management IPv4 address 40
mirror port, configuring 95
multicast filtering 65

P

path cost 71, 73, 75
    STA 71, 73, 75
port authentication 109
port priority
    configuring 80
    STA 76
ports
    autonegotiation 45
    capabilities 45
    duplex mode 45
    flow control 45
    mirroring 95
    speed 45
problems, troubleshooting 131

Q

QoS
    configuring 80
Quality of Service *See* QoS

R

restarting the system 123
RSTP 71
    global settings, displaying 72
    interface settings 75
    settings, configuring 72

S

Simple Network Management Protocol *See* SNMP
SNMP 91
    community string 92
    enabling traps 93
    trap manager 93
software
    displaying version 37
Spanning Tree Protocol *See* STA
specifications, software 127

STA
edge port 75, 76
global settings, displaying 72
interface settings 75
link type 76
path cost 71, 73, 75
port priority 76
standards, IEEE 128
STP 71, 72
STP *Also see* STA

T

trap manager 93
troubleshooting 131
trunk
configuration 52, 54
LACP 54
static 52
Type Length Value
See LLDP TLV
See also LLDP-MED TLV

V

VLAN
interface configuration 60
VLANs
802.1Q tunnel mode 63
adding static members 58
creating 58, 62
description 57
displaying port members 59, 63, 64, 67, 69, 70

W

web interface
access requirements 31
configuration buttons 32
home page 32
menu list 33
panel display 33